Privacy, Data Protection, and the Unprecedented Challenges of Ambient Inteligence

Rouvroy, Antoinette

Published in:
Studies in Ethics, Law and Technology

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

Studies in Ethics, Law, and Technology

Volume 2, *Issue* 1 2008 *Article* 3

Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence

Antoinette Rouvroy*

*Information Technology & Law Research Center and Centre de Recherche Informatique & Droit (CRID), University of Namur, antoinette.rouvroy@fundp.ac.be

Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence*

Antoinette Rouvroy

Abstract

This paper identifies the unprecedented challenges that the prospects of an 'ambient intelligence' era (involving the development of the 'internet of things', with wide dissemination of RFID's, ubiquitous computing, 'smart' objects and surveillance devices) raise from the points of view of 'privacy' and data protection. Privacy and data protection are identified, in line with Agre's conceptualization, as complementary and interdependent legal instruments aimed at preserving the individual freedom to build one's own personality without excessive constrains and influences, and to control some aspects of one's identity that one projects on the world. The 'performativity' and the distribution of agency that characterize AmI systems are exposed as transversal concerns that threaten the fundamental value grounding both privacy and data protection laws: respect for individual autonomy. The relevance, applicability and adequacy of the European privacy and data protection legal frameworks to deal with those unprecedented challenges are then assessed. That assessment required the rethinking of the scope and the normative grounds of what is meant by the 'right to privacy.' Privacy, it is argued, is an instrument for fostering the specific yet changing autonomic capabilities of individuals that are, in a given society at a given time, necessary for sustaining a vivid democracy. What those needed capabilities are is obviously contingent both on the characteristics of the constituency considered, and on the state of the technological, economic and social forces that must be weighed against each other through the operation of legislative balancing. Capacity for both reflexive autonomy allowing one to resist social pressures to conform with dominant drifts, and for deliberative abilities allowing one to participate in deliberative processes are arguably among the skills that a vivid democracy needs citizens to have in the circumstances

*Part of the research for this paper has been made in the course of the MIAUCE research project funded by the European Commission. This paper also benefited from discussions held with Yves Poullet, Christophe Lazaro, Denis Darquennes, Claire Lobet-Maris, Nathalie Grandjean, of the Information Technology and Law Research Center (CRID) and the Center for Technology Assessment (CITA) of the University of Namur, and with Paul De Hert, Mireille Hildebrandt, Serge Gutwirth, Niels Van Dijk, Katia de Vries and Els Soenens of the Center for Law, Science, Technology and Society Studies (LSTS) of the Vrije Universitijt Brussel. The author also wishes to acknowledge the thoughtful suggestions received from the two anonymous reviewers, and the invaluable help received from Nancy J. King of Oregon State University, who kindly agreed to read and improve the linguistic quality of the paper. Remaining mistakes and infelicities remain the author's sole responsibility.

of our times. The value of privacy today, it will be argued, resides in the support it provides for individuals to develop those aptitudes. Acknowledging both the 'intermediate' value of privacy, and its 'social-structural' value, the paper aims at clarifying the conceptual intricacies characterizing privacy and data protection, in view of the emerging challenges raised by the exponential development of information and communication technologies on the threshold of an 'ambient intelligence era.' Finally the applicability of the European data protection scheme to the types of data processing involved in Ambient Intelligence, and the compatibility of the technical visions embedded in those systems with the fundamental data protection principles, are critically explored.

KEYWORDS: privacy, data protection, ambient intelligence, European legal framework, deliberative democracy

INTRODUCTION

Inherited from a time when the physical world and the digital world (also called, somewhat misleadingly, virtual) were clearly distinct from each-other, the utopia of freedom in a cyber-space, liberated from both the constraints inherent to the physical world and the traditional authorities, does not appear compatible anymore with the recent and prospective developments of the information society.

The separation between the 'digital' and the 'physical' that supported the dream of freedom in the digital (disembodied) world happens to be gradually contradicted by the increasing inter-penetration of the 'real' and the so-called 'virtual'. Instead of the free, virtual public space dreamed of in the nineties, the Internet has soon been colonized by profit-driven logics and has soon become the privileged operating field for marketers, whereas search engine operators now "affirmatively control their users' expériences. »[1]

Besides the so-called 'Internet revolution', a wealth of technological innovations is gradually reconfiguring and blurring the distinction between private and public spaces and between physical and digital reality. The development and dissemination of RFIDs[2] (Radio frequency Identification Device) embedded in things (computer mice, goods, clothes, travel documents, mobile phones, and even, possibly, human bodies...) and allowing wireless retrieval of information stored on them prefigure an 'internet of things' communicating and interacting through virtually 'invisible' processes.[3] The orientation of research towards the development of 'ubiquitous computing', that is, of pervasive and invisible information systems allowing constant and automatic

[1] See, Eric Goldman, « Search Engine Biases and the Demise of Search Engine Utopianism », *Yale Law Journal of Technology*, 2006, 188-200: « Complaints about search engine bias implicitly reflect some disappointed expectations. In theory, search engines can transcend the deficiencies of predecessor media to produce a type of media utopia. In practice, search engines are just like every other medium—heavily reliant on editorial control and susceptible to human biases. This fact shatters any illusions of search engine utopianism. »

[2] In its Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on « Radio Frequency Identification (RFID) in Europe: steps towards a policy framework » (COM(2007)96 final), the Commission held that « Radio frequency identification (RFID) is a technology that allows automatic identification and data capture by using radio frequencies. The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a micro-chip to any object, animal or even a person, and to read this information through a wireless device. RFIDs are not just "electronic tags" or "electronic barcodes". When linked to databases and communications networks, such as the Internet, this technology provides a very powerful way of delivering new services and applications, in potentially any environment. »

[3] On the development of the RFID technology and its subsequent legal regulation, see Yves Poullet, Antoinette Rouvroy, Denis Darquennes, « Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID », *Cahiers droits, science et technologie*, CNRS, 2008, forthcoming.

recording of events, open the way to the 'spontaneous' adaptation of the environment (ambient intelligence) to the human user's 'needs', inferred from the information gathered by a system combining a variety of sensors disseminated in the user's environment and processed according to algorithms autonomously adapted by the system itself on the basis of the user's constantly refined profile. The technological innovations this paper is concerned with are those roughly oriented towards a vision of 'ambient intelligence',implying, according to the 2003European IST Advisory Group's report,« Ambient Intelligence: from vision to reality»[4]that

"humans will, in an Ambient Intelligent Environment, be surrounded by intelligent interfaces supported by computing and networking technology that is embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials - even particles of decorative substances like paint. AmI implies a seamless environment of computing, advanced networking technology and specific interfaces. This environment should be aware of the specific characteristics of human presence and personalities; adapt to the needs of users; be capable of responding intelligently to spoken or gestured indications of desire; and even result in systems that are capable of engaging in intelligent dialogue. Ambient Intelligence should also be unobtrusive - interaction should be relaxing and enjoyable for the citizen, and not involve a steep learning curve. »

Such a 'vision' requires

« a real time adaptive environment in which most adaptive decisions are taken by machines in a process of machine to machine communication. These decisions are based on what is called autonomic profiling, severely restricting human intervention, while being in need of a continuous and dynamic flow of information. »[5]

Although ambient intelligence, still in its infancy, is merely a "vision" today, recent technological advances have resolutely placed us on the path towards the realisation of that vision. The intensification of data mining[6] and profiling on the web and elsewhere, aimed at predicting individual behaviours and preferences with more accuracy and impartiality than allowed by human

[4] IST Advisory Group's report,« Ambient Intelligence: from vision to reality. For participation in society & business », 2003. ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf

[5] European Network of Excellence FIDIS (Future of Identity in the Information Society)'s study on "Radio Frequency Identification (RFID), Profiling, and Ambient Intelligence (AmI)", http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf

[6] "Data mining" can be defined as a set of operations carried following the statistical method with the aim of establishing, with a certain margin of errors, correlations between specific observable factors. The result is a method of classification of individuals on the basis of observable factors, allowing the prediction of other, not directly observable, facts. See Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, "L'application de la Convention 108 au mécanisme de profilage", Report for the Council of Europe, 2008.

adjudication; the mushrooming of 'intelligent' cctv[7] able to detect specific patterns of the environment, to admonish people exhibiting 'improper' behaviours in both public and private spaces, assisting security guards, the police and law enforcement officials in their tasks of prevention and detection of crime and incivilities; the gradual dissemination of radio frequency identification technology (RFID) in the commercial, health, and security sectors, allowing wireless distant retrieval of information contained on the RFID tags embedded in goods, clothes, or even human bodies; the perspective of physiological and emotional monitoring of employees through systems, such as the one recently developed by Microsoft, which would allow managers to monitor employees' performance through wireless sensors that could read "heart rate, galvanic skin response, EMG, brain signals, respiration rate, body temperature, facial movements, facial expressions and blood pressure"[8] are all contributing to reconfigure human experience, and to change the terms through which one ought to think of power relations in society and of legal balancing of stakeholders' interests. These economic, technological and socio-political developments are transforming the human space into a globalized, mixed digital and physical space, in which the automatic collection, analysis and mining of information about people, objects, places and contexts may well threaten citizens' fundamental rights and liberties.

The question of how the law should intervene to guarantee that technological progress does not result in violations of fundamental rights and fundamental freedoms has been with us for a long time. Any possible answer that may be suggested at a given moment is unavoidably rooted in specific and fluctuating political, technological and cultural assumptions. The aim of this paper is to assess the relevance, applicability and adequacy of existing European privacy and data protection legal frameworks to deal with the unprecedented challenges carried by the technical visions and the potential industrial application scenarios involved in the current research and development projects in the field of "ambient intelligence". The unprecedented challenges all relate to the unequaled, 'normative' character of these new technologies[9]: the new information,

[7] 'Intelligent cctv', resulting from the growing convergence of previously separated technologies, leading to the production and dissemination of artifacts combining video cameras with facial recognition softwares, 'talking' cameras able to admonise individuals whose behaviours are interpreted as dangerous, suspicious, socially inacceptable or criminal.

[8] For a description of the technological dispositive developped by Microsoft and called "Monitoring Group Activities", see the description provided in support of the patent claim filed: http://appft1.uspto.gov/netacgi/nphParser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220070300174%22.PGNR.&OS=DN/20070300174&RS=DN/20070300174

[9] See Bert-Jaap Koops, « Criteria for Normative Technology. An essay on the acceptability of 'code as law' in light of democratic and cosntitutional values. », *TILT Law & Technology Working Paper*, N. 005/2007*; Tilburg University Legal Studies Working* Paper N. 007/2007: « Technology

communication and networking dispositives, converging in ubiquitous computing and ambient intelligence technologies that do not merely offer individuals new tools that potentially reconfigure human experience, they may also, more fundamentally interfere with the process through which individuals come to build their own personality. In other words, they may affect what Foucault called the process of 'subjectivation', which

« enables us to become subjects of these true discourses, which enables us to become the subject who tells the truth and who is transfigured by this enunciation of the truth, by this enunciation itself, precisely by the fact of telling the truth. »[10]

I believe the core ethical and legal question conveyed by the announced 'ambient intelligence era' is, precisely : how should the law preserve the essential conditions for individual reflexive autonomy and self determination against the very strong incentives for anticipative conformity ensuing from constant observation, monitoring and profiling on the one hand, and against the 'dilution' of human agency engendered by the substitution of patterns of distributed intentionality to the present configuration in which human beings, are the exclusive holders of intentionality.

The question this paper aims to address is wether privacy and data protection regimes may have a role to play in preserving human subjectivation in the still virtual circumstances announced by the 'visions' of ambient intelligence.

Philip Agre grasped much of the relation between data protection and privacy in a simple sentence:

". . . control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity."[11]

These two aspects – freedom from unreasonable constraints (from the state or from others) on the construction of one's identity, and control over (some) aspects of the identity one projects to the world – are at the heart of the most crucial concerns arising when considering, from a legal and political point-of-view, the emerging AmI *scenarios*. Concerns for privacy and data protection in the advanced information society and with regards to the nascent 'ambient

---

has always had a certain normative element – it is never neutral. However, since a decade or two, something is changing. With the advent of information and communication technologies (ICT) and the Internet, technology is being used more and more intentionally as an instrument to regulate human behaviour. »

[10] Michel Foucault, *L'herméneutique du sujet*, Cours du collège de France, 3 Mars 1982, Gallimard, Seuil.

[11] Philip E. Agre, Marc Rotenberg (eds.), *Technology and Privacy. The New Landscape*, MIT Press, 1998, p. 3.

intelligence revolution' have been widely reflected in the literature[12], in opinions of consultative bodies[13] and in various research reports on ethical, legal and social issues raised by current visions of AmI.[14] One obvious reason for this is the fact

[12] A comprehensive list of references would be interminable. Among the most famous references are Lawrence Lessig, *Code and Other Laws of Cyberspace* Basic Books, 1999; Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Random House Trade Paperback, 2005; Daniel Solove, Marc Rotenberg, and Paul M. Schwartz, *Privacy Information and Technology*, Aspen Publishers, 2006; Daniel Solove, *The Digital Person: Technology and Privacy in the Information* Age, NYU Press, 2006. Papers include, for example, see Paul M. Schwartz, "Beyond Lessig's *Code* for internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices", *Wisconsin Law Review*, 2000, 743-788; Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2007). "Privacy, identity and security in ambient intelligence: A scenario analysis." *Telematics and Informatics*. *24*(1), 15; Yves Poullet and Jean-Marc Dinant, "The internet and private life in Europe: Risks and aspirations". In *New Dimentions of Privacy Law*, Cambridge University Press, 2006, pp. 60-90; Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy*, 17, 1998; Lisa Austin, "Privacy and the Question of Technology", *Law and Philosophy*, 22, 2003, pp. 119-199-166.

[13] Of particular relevance, at the European level, are the opinions delivered by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up by article 29 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. See in particular the *Working document on data protection issues related to RFID technology*, WP 105, of 19th January 2005, ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf ; the *Opinion on the concept of personal data*, WP 136 of 20th June 2007, ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf - ; the *Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology*, of 28th June 2005, ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf - ; the *Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC*, ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf - ; *Opinion on the Processing of Personal Data by means of Video Surveillance* of 11th February 2004. The European Commission for Democracy Through Law (Venice Commission)'s recent *Opinion on videosurveillance in public places by public authorities and the protection of Human* Rights, of 23 March 2007 (Study No. 404/2006), CDL-AD(2007)014, http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf is also marginally interesting for our purpose, as the study explicitly excludes legal issues arising from the video surveillance of private areas such as banks, casinos, stores, private residential areas. In the United States, the 2007 *Guidelines for Public Videosurveillance: A guide to Protecting Communities and Preserving Civil Liberties*, a Report by the Constitution Project's Liberty and Security Committee, www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf, provides particularly useful information and reflections.

[14] Of particular relevance are the TAUCIS (Technology Assessment of Ubiquitous Computing and Informational Self-Determination) project, funded by the German Federal Ministery for Education and Research, http://www.taucis.hu-berlin.de/content/de/ueberblick/english.php, the European Network of Excellence FIDIS (Future of Identity in the Information Society)'s study on "Radio Frequency Identification (RFID), Profiling, and Ambient Intelligence (AmI)", http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf, the

that the most essential ingredient, so to speak, of envisioned AmI systems, is information about 'users'.[15] The unavoidable cost of entering in an AmI world, and the very condition of possibility of such a world, appears to be the loss of control over personal information: the constitutive ideas of AmI, such as pervasiveness, invisibility of information systems, constant and automatic recording of events etc. render highly implausible that the user will retain control over what and how information is processed. But the reasons that privacy issues are so vividly debated on threshold of an 'AmI era' go well beyond these important concerns for control over personal information (data protection).

The fact is that the visions behind AmI technologies may appear incompatible with the major importance that Western societies place in cultivating and preserving both *individual autonomy* (freedom from unreasonable constraints on the construction of one's own identity[16]) and *political autonomy* (a vivid democracy where a condition for rules and norms to appear 'just' is that they result from democratic deliberation among citizens endowed with individual deliberative autonomy). Why not discuss individual autonomy right away then? Our answer is that, as such, individual autonomy is not a right but an individual capability that is always a matter of degree. The conditions for individual autonomy are so diverse, so subjective in a sense, that no law could really ensure the genuine effectuation of a 'right to autonomy'.[17] Individual autonomy is a stage in the development of a person that she should strive to attain. Individual autonomy, not more than musical talent, artistic gifts, of happiness, is not something that the State, through the law, could ever 'provide' to individuals.

SWAMI (Safeguards in a World of Ambient Intelligence) project, http://swami.jrc.es/pages/index.htm identifying privacy, identity, security, trust and the digital divide as the main (social, ethical and legal) challenges raised by AmI. Also of interest is the commencing PRIAM (privacy issues in ambient intelligence) project funded by the French INRIA.http://priam.citi.insa-lyon.fr/index.php?option=com_content&task=view&id=12&Itemid=26

[15] We will come back later on the highly ambiguous concept of 'user'.

[16] The importance of a private sphere where the individual could enjoy 'insulation' has been famously acknowledged by John Stuart Mill, in *On Liberty,* (Cambridge University Press, 1989 [1859], pp. 8-9), where he suggests that such insulation may be necessary in order to avoid the 'tyranny of the majority': "there needs protection also against the tyranny of the prevailing opinion and feeling, against the tendency of a society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them; to fetter the development, and, if possible, prevent the formation, of any individuality not in harmony with its ways, and to compel all characters and fashion themselves upon the model of its own. There is a limit to the legitimate interference of collective opinion with individual independence: and to find that limit, and maintain it against encroachment, is as indispensable to a good condition of human affairs, as protection against political despotism."

[17] Considering the 'right to autonomy' as a fundamental human right would require justification for any restriction on that 'right' imposed by the parents to their child.

That is the reason why the "right to be autonomous" does not exist as such in the law.

However, despite the law's inability to 'create' or 'guarantee' individual autonomy, showing *respect* for individual autonomy[18], and, as far as possible, providing the conditions necessary for individuals to develop their capacity for individual deliberative autonomy (the individual process of self-governance) and for collective deliberative democracy (the group-oriented process for critical discourse indispensable to a vivid democracy)[19] have become the most fundamental and basic ethical and legal imperatives in contemporary western societies, where respecting these imperatives is perceived as a precondition to the legality and legitimacy of the law. Individual autonomy and deliberative democracy presuppose a series of rights and liberties allowing individuals to live a life characterized as (in part at least) self-determined, self-authored or self-created, following plans and ideals - a conception of the good - that they have chosen for themselves.[20] Among these fundamental rights and liberties, the *right*

[18] Respect for individual autonomy of persons, and thus for the choices they make, is contingent, in law, to the consideration that the subject is *indeed* autonomous in the choices he or she makes. That condition of autonomy implies the absence of either physical, mental or economic coercion. Legal interference with lawful, fully conscious and uncoerced choices of capable individuals is considered unacceptable, even if interference arises for the sake of the subject's own good, in which case one speaks of unacceptable legal paternalism.

[19] The inspiration for the link between private and public autonomy (the idea that they are 'co-originated' or mutually productive of each-other) is to be found in Jürgen Habermas's discourse theory of law (especially in *Between Facts and Norms*, MIT Press, 1996) according to which "Just those action norms are valid to which all possibly affected persons could agree as participants in rational discourses". One could interpret as an application of this thesis of the co-origination thesis the defense of privacy on the ground of its structural value for society to be read, for example, in Paul M. Schwartz, and William M. Treanor, "The New Privacy", *Michigan Law Review*, 101, 2003, p.216. On deliberative autonomy, see James E. Flemming, "Securing Deliberative Autonomy", *Stanford Law Review*, Vol. 48, N.1, 1995, pp. 1-71, arguing that the bedrock structure of deliberative autonomy secures basic liberties that are significant preconditions for persons' ability to deliberate about and make certain fundamental decisions affecting their destiny, identity, or way of life. On deliberative democracy, see James E. Flemming, "Securing Deliberative Democracy", *Fordham Law Review*, Vol. 72, p. 1435, 2004. Endorsing the concept of a co-originality of private and public autonomy as developed by Jürgen Habermas in *Between Facts and Norms*. On the concept of co-originality, see Rainer Nickel, "Jürgen Habermas' concept of co-originality in times of globaliation and the militant security state", IUE Working Paper Law, 2006/27.

[20] See Onora O'Neill, *Autonomy and Trust in Bioethics (Gifford Lectures, 2001)*, Cambridge University Press, 2002, recalling the wide variety of notions that have been associated to the concept of autonomy by scholars such as Gerald Dworkin (*The Theory and Practice of Autonomy*, Cambridge University Press, 1988), listing liberty (positive or negative), dignity, integrity, individuality, independence, responsibility and self-knowledge, self-assertion, critical reflection, freedom from obligation, absence of external causation, and knowledge of one's own interest as concepts that have been equated to the concept of autonomy, or as Ruth Faiden and Thomas

to individual privacy, understood not merely as a right to be left alone but also as a right to self-determination disallowing paternalism from the state, and the *right to data protection* empowering individuals with means to control the collection, use and disclosure of personal information, on the assumption that lacking such control would subject these individuals to the unbalanced power of others (public authorities or private agents), function as the closest legal 'proxies' to the moral concept of autonomy. As 'proxies' for the legally unattainable moral ideal of autonomy, privacy and data protection are thus often perceived as the most efficient and direct legal instruments to protect individual autonomy on the threshold of a predicted 'AmI era'.

Acknowledgements of the right to privacy as "autonomy in the construction of one's identity" are explicit in the European human rights framework (this is not the case in the United States where the right to privacy has no explicit written constitutional basis except in the context of government intrusions, through the constitutional protection against unreasonable searches and seisures of the fourth Amendment to the US Constitution). Article 8 of the European Convention on Human Rights on the right to respect for private and family life acknowledging that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right to privacy protects individuals against invasions of privacy by public authorities or, through the Convention's horizontal effect, by other individuals,[21] and has been interpreted by the European Court of Human Rights as

---

Beauchamps, *A History and Theory of Informed Consent*, Oxford University Press, 1986, according to whom autonomy may also be defined as privacy, voluntariness, self-mastery, choosing freely, choosing one's own moral position and accepting responsibility for one's choices.

[21] Since the 1981 judgement in *Young, James and Webster v. United Kingdom* (Eur.Ct.H.R., 13 August 1981, Series A No.44) the European Court on Human Rights acknowledges an *horizontal effect* to the Convention, extending the scope of protections to relations between private parties: §49: 'Although the proximate cause of the events giving rise to this case was [an agreement between an employer and trade unions], it was the domestic law in force at the relevant time that made lawful the treatment of which the applicants complained. The responsibility of the respondent State for any resultant breach of the Convention is thus engaged on this basis.' Through this horizontal effect of the Convention, the fundamental rights seem to gain positive effectiveness. The matter is highly controversial, however, just as controversial as the question of the conception of privacy either as a mere *privilege* or as a (subjective) *right*. See also *X and Y v. Netherlands*, 8978/80 (1985) ECHR 4 (26 March 1985), Series A, vol. 91: 'although the object of

including the individual right to control personal information, including in the workplace[22] (the scope of the right to privacy and of the right to data protection may intersect with regards to 'informational privacy'), the right to physical and moral integrity including regarding sexual life,[23] the right to access one's personal records,[24] the right to establish and maintain personal and social life,[25] to establish and develop relationships with other human beings,[26] etc.

The Charter of Fundamental Rights of the European Union[27], reproduces, in its Article 7, §1 of Article 8 of the European Convention on Human Rights to private and family life:« Everyone has the right to respect for his or her private and family life, home and communications. »

Article 8 of the Charter raises the protection of personal data to the status of a fundamental right:

Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.'

[22] See the recent decision by the European Court on Human Rights, in *Copland v. United Kingdom*, 62617/00 [2007] ECHR 253 (3 April 2007), in which the Court held that monitoring of an employee's emails, internet usage and telephone calls had breached the employee's right to privacy. The Court held that even monitoring the date and length of telephone conversations and the number dialed could give rise to a breach of privacy. The arguments of the court included the fact that the employee had not been informed that her telephone calls might be subject to monitoring, and that, at the time, no law exited in the UK that allowed employers to monitor their employees communications. Indeed, the Regulation of Investigatory Power Act of 2000 was not yet in force at that time. The Court does not investigate whether that Act might be inconsistent with the Human Rights Act however.

[23] X and Y v. Netherlands, 8978/80 (1985) ECHR 4 (26 March 1985), Series A, vol. 91.

[24] Gaskin v. United Kingdom, 10454/83 (1989 ECHR 13 (7 July 1989) Series A no. 160. See also Odièvre v. France, 42326/98 (2003) ECHR 86 (13 February 2003), where the ECHR acknowledged that the right to privacy (Article 8 of the European Convention on Human Rights) protects, among other interests, the right to personal development, and that matters relevant to personal development included details of a person's identity as a human being and the vital interest in obtaining information necessary to discover the truth concerning important aspects of one's personal identity.

[25] Beldjoudi v. France, 12084/86 (1992) ECHR 42 (29 March 1992).

[26] Niemietz v. Germany, 13710/88 ECHR 80 (18 December 1992) Series 1, vol. 251 B.: 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he or she chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.'

[27] 2000/C 364/01.

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

The fundamental principles of data protection (fair processing, performed for specific purpose, on the basis of the subject's consent or on other legitimate basis laid down by law, subjective rights of the data subject to access and rectify collected data) has been formalized in the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe,[28] and reiterated in the fair information principles formalised in the European directive on the protection of individuals with regards to the automatic processing of personal data[29] and in the European directive concerning the processing of personal data and the protection of privacy in the electronic communication sector.[30]

The European legal framework of data protection's major instruments are essentially these two important directives : the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[31], and the Directive 2002/58/EC EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.[32] Data protection principles apply to the processing of "personal data" that the directives define as: "any information relating to an identified or identifiable natural person". Except when the data is anonymous or anonymized, any collection, storage and use of coded or personal data relating to human subjects must comply with the 1995/46/EC Directive onthe protection of individuals with

[28] Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of the Council of Europe, ETS No. 108, Strasbourg, 28 January 1981.
[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23 November 1995.
[30] European Directive 2002/58/EC EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.
[31] *Official Journal* L 281, 23 November 1995.
[32] *Official Journal* L 201, 31 July 2002. See also the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending the Directive 2002/58/EC, *Official Journal*L 105, 14 April 2006 P. 0054-0063.

regard to the processing of personal data and on the free movement of such data. When, in addition, that information is about the user's communications on the internet, the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) applies.

The right to privacy (acknowledged in Article 8 of the European Convention of Human Rights and taken over in Article 7 of the Charter of Fundamental Rights of the European Union) and the right to data protection acknowledged at Article 8 of the Charter of Fundamental Rights of the European Union, and implemented by the two Data protection directives) interact in a variety of ways. The European Court of Human Rights has acknowledged that "informational privacy" is among what Article 8 of the ECHR protects. In this regard, data protection directives are among the *tools* through which the individual exercises his right to privacy. More generally, having the guarantee that personal information (personal data) will not be collected and used in manners that totally escape from the individual's control is indeed a precondition for the individual to feel genuinely free from unreasonable constraints on the construction of his identity. Yet, data protection is also a tool for protecting rights other than the right to privacy. Because the data protection directive prevents the processing of information relating to the individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and concerning the individual's health or sexual life, it prevents potential discriminations on these grounds. On the other hand, the right to privacy is irreducible to the right to data protection: it guarantees the inviolability of the home (spatial privacy) ; has to do with the inviolability of the human body ; and protects the individual's emotions and relationships with others. We will come back to those different aspects of privacy later. It is sufficient for now to acknowledge that what privacy protects is irreducible to personal information. Privacy and data protection intersect but are also different tools for enabling individual deliberative autonomy, and, as such, privacy is a precondition to the advent of collective deliberative democracy.

Assessing the requirements that privacy and data protection instruments impose on the design and applications of AmI projects, and identifying the potential inadequacies of the legal framework will be the object of the second section of this paper (Section II). However, some detours are needed as preliminary to these assessments. As privacy and data protection are grounded on the moral imperatives of individual deliberative autonomy and collective deliberative democracy, a precondition to our study of the relevance, applicability and adequacy of legal privacy and data protections in Europe is to identify what, in AmI projects, threatens those fundamental 'autonomic' and 'democratic' values that privacy and data protection are meant to protect. As 'transversal issues'

(Section I), we have identified two main matters in this regard, which are respectively the 'performative' power of the classifications operated by the information systems (I.1), and the increasingly distributed human-objects agency (I.2). Taking these issues seriously, we will argue, requires the development of value-sensitive design or, more precisely, of democracy-sensitive design. Beyond privacy-enhancing technologies, democracy-sensitive design should ensure that socio-technological configurations both *result from democratic deliberation*, and *increase democratic participation and inclusion* (I.3).

SECTION I - TRANSVERSAL ISSUES: ARE AMI SYSTEMS COMPATIBLE WITH PRIVACY AS "FREEDOM FROM UNREASONABLE CONSTRAINS IN THE CONSTRUCTION OF ONE'S IDENTITY"?

The focus of the present section is on how AmI systems, due to their 'performative' power on the one hand, and to the character of distributed agency they exhibit on the other hand, may interfere with the "free development of one's personality", requiring a certain level of immunity from constrains in the construction of one's identity.[33]

I.1 – Freedom from unreasonable constraints in the construction of one's identity and the 'making of people' in AmI systems.

Combined with the ever increasing technological capacities to track, record, analyse, correlate and interpret images, sounds and texts transpiring from human activity and context[34] (through the tracking, recording and analysis of information voluntarily or involuntarily 'released' by the 'users', such as eye fixation, body movements, facial expressions and internet transactions, for example), AmI visions rely on systems capable of 'learning' from occurring events and incrementally self-adjusting to respond optimally to human 'needs' whereas these 'needs', are decreasingly defined by the concerned 'users' themselves, but increasingly defined according to the system's interpretations of whatever happens in the contexts, and of whatever users do or even, increasingly, of what their facial expressions and body motions are. To that extent, one may say that AmI technologies not only rely on the automatic and systematic processing of

[33] Samuel D.Warren and Loouis D. Brandeis explicitly grounded their conception of the "right to privacy" on the peace of mind such a right should allow, and on what they identified as the principle of "inviolate personality", which, according to them, was part of a general right of immunity of the person, "the right to one's personality" (Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", *Harv. L. Rev*. 1890, p. 195 and 215.)

[34] Computing, communication and storage capabilities are said to be doubling every eighteen, six and nine months respectively. (Thomas Skordas and George Metakides, "Major Challenges in Ambient Intelligence", *Studies in Informatics and Control*, 12(2), June 2003.)

personal information, but that they 'construct' and 'produce' knowledge about their 'users'.[35]

The type of knowledge so produced is in no way 'objective' as one has long been able to speak of the 'objectivity' of scientific knowledge. Said otherwise, the information systems involved in AmI visions are not intended to "observe" the unique complexity of each individual human being, but to sort individuals in a variety of heterogeneous categories for the purpose of predicting either their willingness to buy specified commodities, their risk to fill claims with health and disability insurances, the danger they represent for others, or other propensities that marketers, insurers, law enforcement officials and many others will find useful to have. Ian Hacking recently expressed concern with regards to classification of people, which is highly relevant to the assessment of the scenarios envisioned in the field of AmI: when people are taken as objects of scientific or bureaucratic inquiry for a variety of purposes going from controlling to helping them, passing by, organizing them or keeping them away from places, such classifications affect the people classified, and the affects on the people, in turn, change the classifications:

"We think of these kinds of people as definite classes defined by definite properties. As we get to know more about these properties, we will be able to control, help, change, or emulate them better. But it's not quite like that. They are moving targets because our investigations interact with them, and change them. And since they are changed, they are not quite the same kind of people as before. The target has moved. I call this the 'looping effect'. Sometimes, our sciences create kinds of people that in a certain sense did not exist before. I call this 'making up people'".[36]

This 'making up of people' in AmI projects is contingent on the type of finalities and applications of the systems. These finalities and applications are diverse, and very difficult to predict in advance, and will arguably be different depending whether the envisioned applications (or *scenarios*) involve either the "automatic" display of information optimized to the user's needs or preferences as interpreted by the system (e.g. in marketing or interactive web-TV scenarios), or the "automatic" initiation of security measures adapted to the system's interpretation of the events occurring in the environment it captures (e.g. in intelligent video surveillance scenario, with cameras equipped with technologies allowing motion detection, automated tracking, …).

The concerns here are not merely about the increased "visibility" of individual existences in their most tiny details (a concern which was the focus of

[35] The most obvious example of such constructions are the profiles produced through data mining. See Bart Custers, *The Power of Knowledge. Ethical, Legal, and technological Aspects of Data Mining and Group Profiling in Epidemiology*. Wolf Legal Publishers, 2004.
[36] Ian Hacking, "Making Up People", *London Review of Books*, 26(16), 17 August 2007.

the traditional conceptions of privacy)[37], but also about the possibility that *meaning* be ascribed to even the most trivial and fugitive image, sound or movement captured from individuals. The engines involved in AmI scenario are engines of 'discovery' or of 'observation', but also engines for 'making up' people.[38] The probable impacts of AmI *scenarios* consist less in discovering and characterising *what is pre-existing* than it in *creating* new interactions and behaviours involving subjects, objects, and (public and private) organizations, and, through an elaborated interplay of statistics and correlations, in producing, or, more probably, reinforcing the *norms*, the criteria of normality and desirability against which individual lifestyles, preferences, choices and behaviours will be evaluated, with gratifications for compliant individuals, and sanctions for deviant ones, in the form of increased surveillance and monitoring, or of a reduction of access to specific places, goods, services, activities or other opportunities.[39]

The central importance of privacy and data protection in the context of AmI is thus not merely due to the fact that AmI systems record what happens in 'real life'. What is crucial here is that these systems *construct*or *produce* the meaning of those events and, on that basis, frame the user's environment in ways that in turn impact on his self-perception, choices, preferences and behaviours, interfering, potentially at the deepest level, with the effective exercise by individuals of their capacity forself-determination, and with their effective political capacity to participate in the discursive processes of deliberative democracy that should guarantee the justiciability of those classifications.[40]

---

[37] The recent American "Guidelines for Public Video Surveillance" suggested by the Constitution Project's Liberty and Security Committee (2007) acknowledge that "technological advances and social changes have ushered in new and more pervasive forms of public video surveillance with the potential to upset the existing balance between law enforcement needs and constitutional rights and values. Modern public video surveillance systems consist of networks of linked cameras spread over vast portions of public space. These cameras can be equipped with technologies like high resolution and magnification, motion detection, infrared vision, and biometric identification – all linked to a powerful network capable of automated tracking, archiving, and identifying suspect behavior."
(http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf)

[38] See Ian Hacking, "Making Up People", *London Review of Books,*, 17 August 2006, p. 23, where he develops a parallel reflexion, not about AmI technologies, but about humans sciences (many social sciences, psychology, psychiatry and a good deal of clinical medicine).

[39] « Things have changed since Orwell's time, and consumption for the masses has emerged as the new inclusionary reality. Only the minority, the so-called underclass, whose position prevents them from participating freely in consumption, now experience the hard edge of exclusionary and punitive surveillance." (David Lyon*, The Electronic Eye: the Rise of Surveillance Society*, University of Minnesota Press, 1994.)

[40] On the idea that 'profiles' should be made 'justiciable', see Mireille Hildebrandt, "Profiles and Correlatable Humans", in: Christoff Henning, Nico Stehr and Bernd Weiler (eds.), *Knowledge and the Law. Can Knowledge be Made Just?*, New Jersey: Transaction Books 2007.: "If the

Needless to say, to the extent that these classifications condition access or denial of access to valuable opportunities in life, they should result from a democratic deliberative process. Recalling how Lewis Mumfort, back in 1964, characterized democracy may well provide useful inspiration in the circumstances of our times:

"Democracy consists in giving final authority to the whole, rather than to the part; and only living human beings, as such, are an authentic expression of the whole, whether acting alone or with the help of others. Around this central principle clusters a group of related ideas and practices (...). Among these items are communal self-government, free communication as between equals, unimpeded access to the common store of knowledge, protection against arbitrary external controls, and a sense of individual moral responsibility for behavior that affects the whole community. All living organisms are in some degree autonomous, in that they follow a life-pattern of their own; but in man this autonomy is an essential condition for his further development. We surrender some of our autonomy when ill or crippled, but to surrender it everyday on every occasion would be to turn life itself into a chronic illness. The best life possible (...) is one that calls for an ever greater degree of self-direction, self-expression, and self-realization. In this sense, personality, once the exclusive attribute of kings, belongs on democratic theory to every man. Life in its fullness and wholeness cannot be delegated."[41]

At a time where respect for individual autonomy has become the most fundamental and basic ethical and legal imperative, the truly "poïetic" nature of AmI visions is problematic. The "performativity" of the knowledge constructed about users on the basis of correlated data transforms the subjects about whom that knowledge is constructed. From there on, the user's position as « subject » becomes prone to turn into a position as « object ».

A word of caution is needed about the concept of *user*, which is very common in the literature about ambient intelligence and ubiquitous computing, but has never received any thorough definition. It is usually employed to designate the *persons about whom information is recorded and processed*. They may be ordinary civilians in security scenarios, they may be customers in marketing scenarios,… from the point-of-view of data protection, they would be called the 'data subjects', but the reseachers and industrials involved in the development and promotion of AmI appear reluctant to use the term 'subjects'. The same reluctance has appeared in the context of biomedical research where "the research community is slowly beginning to change the language of involvement in biomedical research by patients and the general public. Research

knowledge produced by profiling practices entails exclusion, stigmatisation, confrontation, customisation and even de-individualisation, the question is how to constrain these practices in order to make the knowledge they produce just."

[41] Lewis Mumford, « Authoritarian and Democratic Technics », *Technology and Culture*, 5(1), 1964, 1-8.

'subjects' have become research 'participants'".[42] In the AmI context, the terminological ambiguity attests of the ambivalence of technological developments which *assist* people in their daily activities, increasing their performance, enhancing their security in *given* environments and spaces, while also 'producing' truly *new* spaces, called by some 'performative' or 'surveillance spaces', and, arguably, new 'users' as well.[43]

What conditions would guarantee the 'autonomous' character of expressed choices and consents in a performative surveillance space where citizens systematically adapt their behaviours to what is expected from them, where, on the basis of what they have read, or chosen in the past, one-to-one marketing filters the information and offers communicated to them about goods and services available for purchase, thereby confirming them in their 'profile', where, in other words, they are themselves *constituted* as subjects through their active participation to the system they are asked to consent to? When individual desires, preferences, and choices are always already framed by the technology, when, in other words, no *elsewhere* exists from where individuals could contest what is proposed or imposed on them through the AmI technologies, how can individual autonomy be preserved?

I.2 – Freedom from unreasonable constraints in the construction of one's identity in a context of distributed agency.

The trope of the 'user' may thus be somewhat misgiving to the extent that it conveys the idea of active agency. Although AmI systems are mostly described as 'human centred', as 'reactive' to human choices, actions and needs, and as oriented towards *empowering 'users'* by increasing convenience and entertainment for them, sparing them time and costs, increasing their safety and security, the vocation of AmI systems is to be seamless and disappear from human consciousness, thereby *bypassing users' intentionality and control*, relieving individuals from making decisions and performing certain actions.

To the extent that users are free to use the intelligent interface, they are in part pre-defined in their choices and preferences by the design of technology. "Objects make subjects", Lucy Suchman[44] recently explained, elaborating on the theme developed previously by Madeleine Akrish:

---

[42] Alastair V. Campbell, "The Ethical Challenges of Genetic Databases: Safeguarding Altruism and Trust", *King's Law Journal*, 2007, 18, pp. 227-245: 241.

[43] John E. McGrath, Loving Big Brother: Performance, Privacy, and Surveillance Space, Routledge, 2004. See also, Henri Lefebvre, The Production of Space, Blackwell, 1991.

[44] Lucy Suchman, *Human-Machine Reconfigurations : Plans and Situated Actions*, Cambridge University Press, 2d.ed., 2006.

«Designers define actors with specific tastes, competences, motives, aspirations, political prejudices, and the rest, and they assume that morality, technology, science and economy will evolve in particular ways. A large part of the work of innovators is that of *inscribing* this vision of (or prediction about) the world in the technical content of the new object. I will call the end product of this work a 'script' or a 'scenario.'"[45]

And the 'vision of the world' in contemporary Europe carries a wealth of unchallenged assumptions, such as that carried by the 'security imperative' and the 'efficiency imperative' on which we will return later on. Suffice to say, for now, that the embodiment of these imperatives in the design of technology tends to insulate them from public debates and possible contestation. This may be seen as an interference with the ideal of deliberative democracy.

Design may also interfere with individual deliberative autonomy. Framing the concept of 'technical paternalism', Spiekerman and Pallas[46] suggested that it differs from human paternalism in two important ways. First, machines react automatically and autonomously, which leaves users little room for anticipation or reaction. Second, technology paternalism is not a matter of obedience as it is the case with human interfaces. Instead it is a matter of total compliance, as, by their 'coded' rules, machines can become 'absolute' forces and therefore may not be overrulable anymore (Spiekerman and Pallas provide the example of sensors in a car detecting alcohol on someone's breath, and preventing the car from starting, even in cases of emergency), as, "in a world of Ubicomp, most decisions are performed in the background and are often neither noticed nor can they be reviewed or overruled constantly." Notice of action, which would be necessary for allowing users to overrule decisions made by the machine, indeed appears to contradict the 'calmness' of ubiquitous computing and ambient intelligence.

IBM's vision of 'autonomic computing'[47] radicalizes the idea of non-human agency or of 'cooperating objects' through a systemic view of computing modelled after a self-regulating biological system, that would 'know itself', comprising components that also possess a system identity, be able to configure and reconfigure itself under varying and unpredictable conditions, would always look for ways to optimize its workings, would be able to recover from routine and extraordinary events that might cause some of its parts to malfunction, would be able to protect itself, would know its environment and the context surrounding its activity, and adapt its actions accordingly, would exist with and implement open standards, and would anticipate the optimized resources needed while keeping its complexity hidden.

---

[45] Madeline Akrich, "The De-Scription of Technological Objects", in. W.E. Bijker and J. Law, *Shaping Technology / Building Society*, MIT Press, 1992, p. 208.

[46] See Sarah Spiekermann and Franck Pallas, "Technology paternalism – wider implications of ubiquitous computing", *Poiesis Prax*, 4, 2006, 6-18.

[47] http://www.research.ibm.com/autonomic/manifesto/

A fundamental challenge raised by the new cooperation between humans and objects will thus be for the law to deal with this new form of "distributed agency". Indeed a truly revolutionary feature of AmI is that they are systems where the individual sentient human being loses the exclusivity of "agency" he has traditionally enjoyed, at least from the point-of-view of law. Sociologists, such as Bruno Latour[48], Michel Callon[49] have acknowledged nonhuman agency in actor-network theory. Media artists have understood their poetic potential - that is, the potential they offer to imagine and create radically different spaces – and, relying on new information, communication and networking technologies, have begun indeed to "create" new spaces, new experimental experiences.[50] But from the legal point of view, the spread of agency is resented as a true disruption. One reason for this is that the presumption that only sentient human beings exhibit 'agency' is fundamental to the law's capacity to assign individual responsibility and liability.

This raises fundamental and very basic questions with regard to the functioning of law in a world of AmI: how shall legal responsibility be allocated for the potential harms and violations of rights when intentionality is 'spread' and not exclusively locatable in individual psychism? How to assign responsibilities in computer-controlled environments where it becomes impossible to locate and isolate the cause of potential damages resulting from combined agencies originating from computer hardware and software, networks, and human beings?[51] How can meaning be ascribed to the 'informed consent' provided by

[48] Bruno Latour, Reassembling the Social: An Introduction to Actor-Network-Theory, Oxford University Press, 2005.

[49] Michel Callon, "Les réseaux sociaux à l'aune de la théorie de l'acteur-réseau", *Sociologies Pratiques*, n.13, pp. 37-43, 2006.

[50] See Sha Xin Wei, "Poetics of performative space", *AI & Society*, 21(4), June 2007. See also the Planetary Collegium / Montreal 2007 Summit, "Reviewing the Future: Vision, Innovation, emergence", 19-22 April 2007 (abstracts viewable at http://summit.planetary-collegium.net/abstracts.html). Another example is *Alternet Fabric*, a private company composed of Architects, telecommunication and computer scientists and artists engaged in common architectural, esthetic and technologic projects (http://www.fabric.ch).

[51] See Hilty et al. *The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment*, Swiss Center for Technology Assessment (TA-SWISS), Bern (TA46e/2005) and Scientific technology options assessment at the European Parliament (STOA 124 EN). http://www.ta-swill.ch/www-remain/reports_archive/publications/2005/050311_STOA125_PvC_72dpi_e.pdf
p. 17 : « As a rule, it is not possible to isolate the cause of damage due to the combined effects of several components from computer hardware, programmes and data in networks, as no one can cope with the complexity of such distributed systems, neither mathematically nor legally. As society's dependence on systems of this kind will grow with Pervasive Computing, a net increase in the damage derived from unmastered technical complexity has to be expected. As a consequence, a growing part of day-to-day life will, virtually, be removed from liability under the causation principle. »

individuals to the electronic treatment of personal data when individual preferences are from the outset framed by the norms of the 'infosphere'? We will come back to those questions later on. For now, simply, acknowledge that the 'performative' power of AmI over individual desires, choices, preferences and behaviours, and the distribution of agency in AmI set unprecedented challenges for the law.

An important challenge for the law in advanced AmI environments, but also in more modest visions encompassed in early projects developing pieces of technologies that might later be implemented in AmI systems, will be to deal with the increasing dissociation between the concept of 'users' and that of 'agency'. Empowerment of 'users' through the mechanisms described in fair information principles formalized in the European data protection framework may only partially resolve the issue, as will be further explained in the next section. Advanced information and communication technologies are partially outpacing current legal protections of personal data and privacy in several ways, of which the confrontation of the technological visions embedded in the AmI systems with the fundamental principles of data protection and privacy provide many examples. To these challenges, the law does not necessarily have pre-determined, definitive and secure responses. Guarantees of fundamental rights and liberties in a world of ambient intelligence will not be found nor constructed by the law alone: it is now commonsense that the law alone, however well thought through and drafted, is ill equipped to provide exhaustive and sufficient responses to the normative and regulatory challenges of the advanced information society.

In assessing the aspects, scope and value of privacy and data protection that are pertinent in the context of AmI (Section II), we will need to take those transversal concerns into account, as well as to acknowledge that privacy and data protection will have to rely on much more than law for their protection. A new regulatory metabolism, including law, technology and social deliberation will need to be activated.

I.3 – A lesson from the transversal challenges? Towards a democracy-sensitive technological design.

The legal challenges of AmI visions are further complicated by the ubiquitous and "pleiotropic" characters of the emerging technologies, that is, respectively, their potentiality to be embedded in any object of our environment (cf. RFID tags) or even in the human body itself, and their capacity to develop in a multitude of unpredictable applications. That AmI-related technologies may be developed into a wide variety of unpredictable scenarios makes prospective legal inquiry intricate and renders it very difficult for the law to usefully regulate these developments *a*

priori.[52] It is reasonable to assume that the law may have to evolve to accommodate the new challenges raised by AmI, but although the path followed by legal change is usually *evolutionist* (following a method of anchoring and adaptation), the unprecedented character of some of the issues awaiting regulation in a world of ubiquitous computing and ambient intelligence might well render former anchors irrelevant.

Besides those methodological difficulties, the uncertainty and variety of potential applications (scenarios) has implications for more than one branch of law. Let us take, for instance, intellectual property law: a very practical problem soon to be confronted in this regard relates to the adaptation of intellectual property policies to individual innovations that are at the same time finalized inventions, and components embedded into other technological products or daily use objects. Allocation of patents on, say, RFIDs, allows private constructive pre-emption of the new AmI space. The impact of IPRs as incentives or disincentives to innovate must be assessed anticipating the wide variety of undefined, unpredictable scenarios involving convergent technologies and the development of an "internet of objects". Patents in this context are not merely about rewarding technological innovation and, thereby, producing positive incentives for the development of useful technological solutions to technical problems. For example, a patent over a basic technological element that may be involved in complex ambient intelligent networks grants power to the patent holder to orient the very construction of the "AmI ecosystem" (the vision of AmI implies that the human-digital interface indeed appear "natural"), a power that is not merely technological, but also highly political by nature: it is essentially a power over the political economy of information environments.

From the transversal issues described above and from the new complexities facing legal regulation of unpredictable technological developments, it is undeniable that policy and technology have become increasingly interdependent.[53] Legal principles, to be efficient, may need to be "embedded" in the technology itself (the development, encouraged by the European Commission,

[52] See also Kevin D. Werbach, "Sensors and Sensibilities", *Cardozo Law Review*, 2007, 28(5): 2321-2372, arguing that the fact that sensors will be embedded in the most trivial objects used in daily life will make it difficult for the law to regulate AmI technology itself: it would make it difficult or either impossible or enormously costly to either ban them altogether, restrict their use in specific circumstances, restrict specific uses of those devices, or even try to shape how the technology operates, as the devices in which it is embedded may be general-purposes devices.

[53] James X. Dempsey and Ira Rubinstein, "Lawyers and Technologists. Joined at Hips?", *IEEE Security and Privacy*, May/June 2006, pp. 15-19. See also Paul M. Schwartz, "Beyond Lessig's *Code* for internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices", *Wisconsin Law Review*, 2000, p.787: "a central fashion in which regulation takes place in cyberspace is through "code", that is, through technological configurations and system design choices."

of privacy-enhancing technologies (PET's), attests of the new distribution of regulating power between law and technology), with the implication that lawyers and engineers must engage in dialogue,[54] and also that democratic debates should take place regarding *what this will change*. To illustrate, what was 'merely' legally prohibited may become technically impossible. What are the consequences are of making it technically impossible to contest a legal prohibition in court by making that prohibition technically impossible to breach in the first place ?

The development of *value-sensitive* design in pervasive and context-aware information and communication systems requires "design guidelines that are both specific enough to provide meaningful direction and sufficiently flexible to be used across systems and deployment conditions".[55] As the current research and development projects in information and communication technology are the precursors of a technological revolution expected to crucially affect human experience and performance in both trivial and important behaviours and interactions constitutive of our economic, politic, cultural, social and intimate daily life, these design guidelines should moreover be *democracy-sensitive*, in the sense that they should themselves *result from democratic deliberation*, and *increase democratic participation and inclusion*. "Inventors" of AmI technologies cannot be characterized simply as problem-solvers ; the technology they develop is not simply aimed at solving problems that simply exist "out there". They are also, "constructing" bundles of solutions who construct problems suited to their

[54] See Lawrence Lessig, "The Architecture of Privacy", *Vanderbilt Entertainment Law and Practice*, 1, 1999, and *Code and Other Laws of Cyberspace*, Basic Books, 2000 where Lessig, advocating mixed property-based and technological solutions to the issue of privacy on the Internet, suggests to structure privacy rules along a two-tier mechanism involving, on the one hand, acknowledgement that each individual has property interest in her own information and, on the other hand, the use of software transmission protocols to empower the individual with the possibility to control her access to the web-sites according to her privacy preferences and the extent to which each site's practices meet meets those preferences. For a critique of Lessig's approach, see Paul M. Schwartz, "Beyond Lessig's *Code* for internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices", *Wisconsin Law Review*, 2000, 743-788. Besides the argument that most users will probably never master and/or use the software transmission protocols (such as P3P), Schwartz criticizes Lessig's idea that privacy protects a right of individual control, and rather suggests that privacy is a constitutive value that safeguards participation and association in a free society. Schwartz identifies the normative function of privacy as inhering in its relation to participatory democracy and individual self-determination. While he recognizes that a privacy market may play a role in helping information privacy fulfill its constitutive role, Schwartz considers that shortcomings and structural difficulties in that market make it improbable that those market failures can be spontaneously solved by the market itself. His recommendation is thus to rely on fair information practices, that he conceptualizes as a mixture of property and liability rules, with mandatory and default elements.

[55] Anne Jacobs, "The benefits of The Legal Analytic Perspective For esigners of Context-Aware Technologies",
guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/UbicompPaper2.doc

unique skills and ideas"; they "invent both artifacts and frames of meanings"[56] and should therefore acknowledge the fundamentally political nature of their work.

SECTION II – RELEVANCE, APPLICABILITY AND ADEQUACY OF THE EUROPEAN PRIVACY AND DATA PROTECTION LEGAL FRAMEWORKS TO THE UNPRECEDENTED CHALLENGES IN AMI.

Our orientation in thinking about privacy and data protection in a context of ambient intelligence is to consider the scope, meaning and value of those rights in a contextualized and pragmatic manner rather than in a purely positivist way. Law is 'not a tangible object of the real world', but a 'concept or process'.[57] That one needs to be able to identify *what it is, in each context*, that privacy and data protection protect in order to balance privacy and data protection principles against competing principles and legitimate interests, may appear a truism, but a truism that most positivist legal scholarship appears to forget, failing to assess, behind positive laws, the extra-legal values promoted. An important task in assessing the relevance, applicability and adequacy of the European privacy and data protection legal frameworks is to distinguish, as separate issues, the scope (aspects of privacy), the values (or normative grounds) of privacy, and the instruments of privacy and data protection. The abundant literature on privacy rarely makes those distinctions explicit, and, as a result, sometimes obscures rather than clarifies what indeed is meant by the legal concept of "privacy" in the advanced information society.[58]

It is only through consideration of the nature of the threats that the new information and communication technologies raise for a free and democratic society that one may identify the type of privacy protections needed in the current

[56] W. Bernard Carlson, "Artifacts and Frames of Meaning: Thomas A. Edison, His Managers, and the Cultural Construction of Motion Pictures", in. Wiebe E. Bijker, J. Law, eds., *Shaping Technology/Building Society. Studies in Sociotechnical Change*, pp. 175-176.

[57] L. Friedman, *Law and Society. An Introduction,* Prentice Hall, 1977, p. 3.

[58] Serge Gutwirth and Paul De Hert, usefully make those distinctions. One agrees with their suggestion that privacy is a *tool* that shield individuals against others' interferences, and regret, with them, that, as far as data protection is concerned, transparency seems to have replaced legitimacy as the core *value* of data protection. (Serge Gutwirth, Paul De Hert, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Erik Claes, Anthony Duff and Serge Gutwirth, *Privacy and the Criminal Law*, Intersentia, 2006.) That indeed the 'legitimacy' imperative of data processing is not sufficiently assessed by Courts may in part be explained by the pression that the 'absolute logics' of security and efficiency impose on any proportionality test that one might wish to implement in assessing the legitimacy of data processing.

configuration of our society and for the future.[59] The legal concept of privacy we need in a world of ambient intelligence will not necessarily be the same concept as the one we needed in a pre-information society. In the pre-information society, local social norms (like norms of decency regulating what people were allowed to disclose or not in public), strong physical and temporal boundaries (like walls and the limitation of human memory), a framing of issues of security and efficiency different from the one experiences nowadays (with security and efficiency largely imposed as absolute logics trumping other considerations), and the fact that personal information was not yet considered, as it is today, as a basic resource of informational capitalism[60] (no "market" for personal information existed), privacy laws protecting only intimate matters and sensitive information were arguably playing their role satisfactorily in view of maintaining the free and democratic characteristics of society.

As Lisa Austin argues, however,

"because technology creates privacy issues that fall outside the bounds of our traditional analysis – known and even accepted surveillance, collection of non-intimate information, collection of information in public – we do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations." [61]

Sharpening and deepening our understanding of traditional concerns regarding privacy and data protection is what is attempted in the following pages.

II.1 - The right to privacy

II.1.1. The scope of privacy.

AmI technologies have the potential to increase the 'visibility' of the wide range of daily experiences that compose the fabric of everyday life and that, for a significant part, we never even had to think of as 'private' or 'anonymous',[62] as

[59] Article 1 of the "Data protection directive" (95/46/EC) explicitly frame data protection in the larger context of the protection of fundamental rights and freedoms: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

[60] Perri6 (1998) *Private Life and Public Policy* in *The future of Privacy: Public Trust in the Use of Private Information v. 2*, Lasky, K and Fletcher, A (eds), Demos Medical Publishing: "what is distinctive about informational capitalism is that personal information has become the basic fuel on which modern business and government run and (…) the systematic accumulation, warehousing, processing, analysis, targeting, matching, manipulation and use of personal information is producing new forms of government and business (…)."

[61] Lisa Austin, "Privacy and the Question of Technology", *Law and Philosohpy*, 22, 2003, p. 164.

[62] Anonymity has been described famously by Alan F. Westin as a form of privacy "that occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance" (*Privacy and Freedom*, Athenaeum, 1967.) Anonymity is

there were no reasons to fear being 'watched', recorded and interpreted by others, either because the technical capabilities to do so were lacking, or because we thought those experiences were so trivial and meaningless that nobody would ever pay attention to them.

A useful question to ask is: what aspects of our life are protected when we 'have' privacy? Spatial, informational, emotional, relational, communicational privacy are various 'aspects' of privacy with which AmI technologies may interfere.

Communicational privacy is explicitly acknowledged in Article 8 of the European Court of Human Rights and in Article 7 of the European Charter of Human Rights, and suggests the enjoyment of a certain level of intimacy when one communicates with others, even in the public space, as well as a guarantee of some confidentiality of the content of our communications with others.

We can moreover feel 'privacy' when we have our 'spatial' territory, such as our home, protected from unconsented intrusions by others. Protection of the home is indeed explicitly acknowledged in Article 8 of the European Court of Human Rights and in Article 7 of the European Charter of Human Rights. Ubiquitous and pervasive computing easily crosses walls, and has the potential to interfere with our *spatial privacy.*

We also share the notion that our own body should be protected from intrusive gazes. The reason why we wear clothes is not exclusively the need to protect ourselves from the cold or from the sun. There is something more: *physical privacy* (in the American Constitution, protection against unwarranted searches and seizures protects, to a certain extent, the physical privacy of the citizens). In this regard, protection of the legitimate interests of individuals may require reconsidering the "boundaries" of the subject. The European Group on Ethics of Science and Technologies suggested, in its 2005 report on ethical aspects of ITC implants in the human body, a broader conception of the individual endowed with the right to claim the total respect of a body, which is at the same time physical and virtual. The idea has been suggested, for a few years already, (and especially in feminist and post-structuralist scholarship), that the person, the subject deserving legal protection, is irreducible to the spatially situated and physically circumscribed subject.[63] Disembodied informational samples gathered

---

certainly something most people expect to have even in public places, although, as it will be argued, because expectations of privacy and anonymity are indeed inversely proportional to the intensity of surveillance, those expectations are probably prone to decrease in the coming years, if the 'security state' further develops.

[63]See Haraway, D J (1997) Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience, Routledge, p. 247) : 'Most fundamentally,(…) the human genome projects produce entities of a different ontological kind than flesh-and-blood organisms (…) or any other sort of "normal" organic being (...) the human genome projects produce ontologically specific things called databases as objects of knowledge

in databanks, in that view, constitute 'informational identities'[64] parallel to – but interacting with - the physically embedded identities, and independent from the personal biographies through which individuals construct and maintain their self-perception. How 'physical privacy' interacts with the potential legitimate interests that a person has in the protection of his or her 'digital' or 'virtual' identity would be an interesting field of research.

Informational privacy is a notion that appears quite obvious to most people, although they are not necessarily conscious that images, sounds, movements 'emanating' from their body are indeed at stake when they think of informational privacy. The usual way to protect informational privacy is by empowering the subject with (legal and/or technical) means to control the collection and use of personal information.

Privacy may also be conceived as protecting one's "thoughts, emotions, and sensations"[65] and thereby one's "right to inviolate personality". The tracking and analysis of facial expressions in order to derive information about "users"'emotions obviously interferes with the enjoyment of *emotional privacy.*

As has already been mentioned, the European Court of Human Rights acknowledged that the right to privacy is not something that must necessarily be lived in isolation: the right to enter in relationships with others, or the right to *relational privacy*, is part of the right to privacy. This is not surprising if indeed one understands the right to privacy as the right to construct one's personality free from unreasonable constraints. Relations with others are essential to the construction of an individual's personality. Respect for relational privacy may require others to abstain from interfering with the personal relationships.

That legitimate interests of privacy may be acknowledged in those, and many other, diverse dimensions of human existence does not necessarily imply that those interests always trump competing interests of others (the government, enterprises, other individual). It is the law's business to balance these legitimate interests of the subject against the competing interests of others to interfere with his 'privacy'. Several methods exist to this end.

In the United States, the Supreme Court has repeatedly conditioned her acknowledgement of the existence of a right of privacy in specific area of human life to the existence of 'reasonable expectations of privacy' in those areas. The major weakness of such a method is that the generalization of surveillance

---

and practice. The human to be represented, then, has a particular kind of totality, or species being, as well as a specific kind of individuality. At whatever level of individuality or collectivity, from a single gene region extracted from one sample through the whole species genome, this human is itself an informational structure.'

[64] See Katja Franko Aas, "The body does not lie' : Identity, risk and trust in technoculture*", Crime, Media, Culture*, 2006, 2(2):143-158.

[65] Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harv. L. Rev.* 1890, p. 193.

devices, especially in the public space, decreases the public's expectations of privacy anyway. It is not useless to recall that although 'expectations of privacy' do not play such an important role for the definition of the right to privacy in Europe, the decrease of expectations of privacy will necessarily negatively impact the probability that people will indeed claim respect of their right to privacy in those new areas where they are 'observed', as well as reduce the likelihood that people will refuse their consent to being 'observed'. Preserving awareness about issues of privacy may be both of paramount importance and enormously challenging the more we progress in the surveillance society. A theory of privacy relying on 'expectations of privacy' cannot more be justified by saying that what privacy is about is the right individuals have not to be 'surprised' by surveillance devices they ignored to be there. Even where people know they are observed, and thus have no expectation of privacy because they have been informed that surveillance devices are in use, surveillance, even overt, and not hidden, may cause people harms that they would probably describe as invasion of their privacy. The most unsophisticated example of this would be an instance where video cameras have been placed in public toilets. More subtle instances would be, for example, instances where employees would know they are being monitored by their employer and their productivity evaluated in real time. Although they do not have expectations of privacy in that case, they still have lost something that resembles very much 'their privacy'.

Another method, more usual in Europe, for balancing competing interests and establishing whether or not, in each situation, there is a right to privacy or not, and whether or not legitimate and sufficiently compelling reasons exist for allowing interferences with that right, is normative inquiry.

II.1.2. The normative grounds of the right to privacy.

The normative grounds of privacy are logically contingent on the type or aspect of privacy that is being considered. For the purpose of this paper, although we acknowledge that other aspects of privacy are obviously involved in the *scenarios* potentially ensuing from AmI systems, we will restrict our inquiry to informational privacy.

II.1.2.1. Powerful political, economic and cultural forces militate against informational privacy.

Some of the fundamental assumptions shaping both the technological and legal developments of the day are inextricably bound within the fabric of our current political economy. They form and are formed by the political, economic, and social context that commands the development of the information society.

The current support for, and massive investment in, the development and intensification of the information society (where the term 'information' refers essentially to 'personal information', as the new technological devices developed are essentially constructed as to channel personal information about individual citizens, patients, suspects, consumers from those individuals to public authorities, government officials, commercial enterprises, managers), is (in part) derived from, and in turn (in part) reinforces, two simultaneous evolutions: the advent of the *security imperative* on the one hand, and the *individualization of risks* in the neo-liberal societies on the other hand.

a) The security imperative.

A first evolution relates to the *security imperative* that has become an absolute logic, in both law enforcement and, to a lesser extend, socio-economic relations, trumping all other considerations and is therefore absolved, to a large extent, from proportionality tests. In this logic, the entirety of human behaviours and interactions are subjected to control and scrutiny. The logic of security, because it is absolute by nature, does not tolerate the competing claims of privacy. [66]In the context of law enforcement, Rainer Nickel notes

"the shift from enabling 'freedom' to upholding 'security' as the central description of the function of the nation-state. This shift has severe implications for the discourse on human or constitutional rights and their a priori status as a constraint on the popular sovereign: from infinite detention, through (bio) data collections on an unprecedented scale, to the use of torture,and from pre-emptive shootings of suspects and kidnapped or suspicious passenger planes to pre-emptive wars, the security paradigm seems to trump the traditional notion of inalienable individual rights and replace them with the rule that the end justifies the means."[67]

In that 'security paradigm', clams to have one's privacy respected is less perceived as the exercise of a fundamental right than as a way for those who claim to have their privacy respected to try hiding a wrong. To a certain extent, the anti-privacy rhetoric used to sustain the "security paradigm" is the same as the anti-privacy rhetoric used by law and economics scholars such as Posner and Epstein, seeing personal privacy not as a final value, but merely as an instrument

[66] See Institute for Prospective Technological Studies – Joint Research centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE)*, July 2003, IPTS Technical Reports Series, EUR 20823 EN, 97. See also Hardt, M. et Negri, A., (2004) *Multitude. Guerre et démocratie à l'âge de l'empire.* La Découverte, pp. 240-246.

[67] Rainer Nickel, "Private and Public Autonomy Revisited: Jürgen Habermas' Concept of Co-Originality in Times of Globalisation and the Militant Security State", EUI Working Paper, Law No. 2006/27.

used by dishonest people to deceive others,[68] under the assumption that honest people do not have reasons to value their privacy.

In the socio-economic context, the most radical law and economics theories, prolonging utilitarian theories, ground their arguments against any form of regulation restricting access to personal information by market agents, on the idea that protecting an individual right to privacy, and allowing individuals to 'lie' in the socio-economic exchanges, undermines the common good, understood as the aggregate welfare in society. « People should not - on economic grounds, in any event - have a right to conceal material facts about themselves », Posner argues.[69] Allowing people to conceal personal information relating to things such as 'arrest records, health, credit-worthiness, marital status, sexual proclivities' would likely result in people concealing discreditable facts about themselves with the aim of selling their services or involvement at an improperly high price.[70] Those who

« profess high standards of behaviour in order to induce others to engage in social or business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character."[71]

In its 'law and economics' version, the value of privacy is thus essentially anti-social, instrumental, whereas personal information is a form of 'input into the production of income or some other broad measure of utility or welfare'. Privacy, those authors argue, should be protected only when it increases wealth and social utility but should be assigned away from individuals when it does not, and especially as it allows anti-social behaviours. The method developed by Richard

[68] See Richard Epstein, « How Much Privacy Do We Really Want? », *Hoover Digest*, n.2, 2002 and Ruth Gavison, « Privacy and the Limits of Law » in Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, Cambridge University Press, 1984.

[69] Richard A. Posner, 'The Right of Privacy', *Georgia Law Review*, 1978, 12: 399.

[70] Richard A. Posner, 'The Right of Privacy', *Georgia Law Review*, 1978, 12: 393-422; Richard A. Posner, « An Economic theory of Privacy » in Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, Cambridge University Press, 1984. Privacy allows individuals to manipulate access to personal information and therefore the world around them, thereby increasing transaction costs between bargaining parties and creating harmful information asymmetries. Individuals, in that view, are essentially bad persons, whose main aims in life are oriented by their desire to gain unwarranted advantages over others rather than to cooperate with others. For a critique of Posner's views on privacy see Baker, C E 'Posner's Privacy Mystery and the Failure of Economic Analysis of Law', *Georgia Law Review*, 1978, 12(3): 475-496.

[71] As stated by Ferdinand Schoeman, there are numerous grounds for puzzling over the significance and value of privacy. 'The right to privacy is seen as creating the context in which both deceit and hypocrisy may flourish: It provides the cover under which most human wrongdoing takes place, and then it protects the guilty from taking responsibility for their transgressions once committed'. (Ferdinand D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Antology*, Cambridge University Press, 1984.)

Posner for deciding about this assignment of informational privacy consists of a twofold test. The first test consists of an inquiry into whether (1) the personal information is 'a by-product of socially productive activity', and (2) 'its compelled disclosure would impair the incentives to engage in that activity'. Posner's conclusion is that while corporate data and other trade secrets should generally be protected (meaning – under US law - that the employee generally loses control over intellectual property they create at work?[72]), most facts about people should not. Indeed, he writes: "Secrecy is an important method of appropriating social benefits to the entrepreneur who creates them while in private life it is more likely to conceal discreditable facts."[73]

The theory may undoubtedly well increase the power asymmetry between, for example, workers and employers, but it is a common criticism addressed against utilitarianism that it disregards the widely shared taste for fairness.[74]

Richard Epstein, defining his own view in these cases as remaining that of an unrepentant libertarian, viewing employees as having no legitimate interest in the protection of their personal information against the employer, argues that personal information is, after all, nothing more than a commodity that should be allocated according to market rules:

"The employer can ask any question of the prospective employee that she wants. The applicant may refuse to answer. In the end, the two can decide whether the information is more valuable when kept private or when shared. In many cases, the personal life of an employee will be regarded as information to which the employer has no right. If so, it will not be because of some high principle, but because of the joint recognition that the information is worth less to the employer than its concealment is worth for the employee. Let the employee receive comprehensive benefits from the employer, such as health care, and the calculus may well shift radically: now it does matter whether the employee drinks, smokes, or exercises on a regular basis. If that information is relevant to an insurer in setting risk, then it is relevant to the employer who has to foot the bill for the long-term health plan."[75]

In Richard Epstein' view, and in the view of those taking inspiration from him,[76] privacy of personal information in the workplace should no longer be

[72] On that question, see Catherine Fisk, « Reflections on the New Psychological Contract and the Ownership of Human Capital », *Connecticut Law Review*, 2002, 34 : 765-782.
[73] Richard A. Posner, "The Right of Privacy", *Georgia Law Review*, 1978, 12: 393-422
[74] See W. Farnsworth, "The Taste for Fairness*", Columbia Law Review*, 2002, 102: 1998-2010.
[75] Richard Epstein, "Deconstructing Privacy and Putting it Back together Again", *Social Philosophy and Policy*, 2000, 17(2): 22.
[76]See for example Tom Miller, Director of health Policy Studies, Cato Institute, Testimony on Genetic privacy, before the House Judiciary Subcommittee on the Constitution on genetic privacy, September 12, 2002.: 'Rather than rely on greater regulation of information flows simply because they are labelled genetic, we should restore and renew our commitment to competitive markets, private property rights, and private contracts.'

granted any protection. The presupposition made is that the employer is entitled to know anything about the employee in which it has an interest. No need to say here that such a presupposition, granting employers prima facie entitlements to any private information about their employees, is contradicted by social conventions and certain normative values placing much of the personal life of employees, including facts that may indeed impact on job performance, such as the kind of lifestyle employees have after work hours and during the week-ends, beyond the legitimate concern of employers. Economic relevance of private information does not suspend the normative value of privacy.[77]

According to 'hard law and economics' supporters, however, the transaction costs arising from uncertainties about the genetic status of persons, and information asymmetries existing between the contracting parties, decrease the efficiency of the marketplace, and is thus incompatible with the common good. Some would even suggest that those who create or refuse to abolish a removable uncertainty should be held responsible for the transaction costs associated with the lack of transparency, and should accordingly be charged for those increased costs.[78] Those who want privacy for themselves, refusing thereby to be submitted to the transparency imperative of the market, should thus pay the cost of privacy. In order to be competitive, however, any market trader should take privacy seriously. Respect for consumers' preferences for privacy might become a commercial argument: provision of privacy, on a competitive market, should be beneficial to those agents who provide it when other agents don't (at least if one considers that consumers would usually prefer to be protected in their privacy).

b) The individualization of risks.

Besides this 'security imperative' at play in both the field of law enforcement and socio-economic relations, there are the institutional shifts accompanying neoliberalism and the ensuing social need to ground identification of individuals and predictions of their risks and behaviours on private information, such as health, lifestyle, consumption habits, etc. The compulsive interest for private information, in a perspective that locates the main source of risks in personal characteristics and behaviours, indeed reflects the move western societies are

(http://www.house.gov/judiciary/miller091202.htm#_edn11>)

[77] Restrictions of the type of information insurers or employer scan ask about prospective policy-holders and job applicants are based on that consideration, and may sometimes be viewed as indirect ways to implement redistributive policy. In the same sense, legal interference with contractual freedom may be a legitimate instrument of redistributive policies. See A.T. Kronman, "Paternalism and the Law of Contracts", *Yale Law Journal*, 1983, 92: 770.

[78] What the law and economics movement teaches us, at least, is that the protection of privacy on the marketplace raises a cost that should be paid by someone.

currently experiencing from the model of the universal insurance society, or welfare state, to the actuarial post-Keynesian society. In the actuarial post-Keynesian society, the two significant attributes are the decrease of individual privacy and the rise of discourses of personal responsibility and personal accountability for bad luck.

A first assumption is that personal information about individuals is the most precious input for the planning and management of governmental and business activities, as it is believed that private information necessarily allows accurate predictions of risks and behaviours and a significant reduction of the costs associated with uncertainty.[79] As a matter of fact, despite the explicit acknowledgement of human rights as "constitutional instruments of the European public order",[80] and the reaffirmation, by Article 6 (ex Article F) of the Amsterdam Treaty, that respect for human rights and fundamental freedoms is part of the grounds of the European Union[81], privacy interests are increasingly trumped by the needs of governments and businesses to use a wide range of personal information about individuals in order to increase security and to minimise transaction costs and other inefficiencies born by informational asymmetries.

As selectivity replaces universality as a principle for the distribution of welfare benefits, discourses of personal empowerment, activation and responsibility induce individuals to assume personal responsibility for most adverse circumstances resulting from 'brute bad luck', for which they would have expected some compensation from the community in a traditional welfare-state. In this way, the concept of 'risk' becomes a privileged disciplinary tool of post-Keynesian governance: it functions as a 'technology of the self', urging individuals to get the most information they can about their personal risk status, to act 'rationally and responsively' after having been so informed, and to take the responsibility to minimize their risks. [82]

Whereas the insurance society typical of the welfare state shifted the focus from the subjective notion of behaviour and individual responsibility to the objective notion of risk as probabilities, and replaced moral assessment of

[79] Julie E. Cohen, « Privacy, Ideology, and Technology: A Response to Je rey Rosen », *Georgetown Law Journal*, 2001, 89 : 2029-2045.
[80] *Loizidou v. Turquie (preliminary exceptions)* ECHR (1995), series A vol. 310, 27 § 75.
[81] Even before the enactment of the Charter of Fundamental Rights of the European Union, the Court of Justice of the European Community protected fundamental rights in its jurisdiction as they are part of the unwritten general principles of community law. See Dean Spielmann, "Jurisprudence des jurisdictions de Strasbourg et de Luxembourg dans le domaine des droits de l'homme: conflits, incohérences et complémentarités", *in. Philip* Alston (ed.), *L'Union Européenne et des Droits de l'Homme*, Bruxelles, Bruylant, 2001.
[82] In this regard see developments in A. Rouvroy, *Human Genes and Neoliberal Governance: A Foucauldian Critique*, Routledge-Cavendish (GlassHouse books), 2008.

individual behaviours by amoral statistics, in the rising post-Keynesian society, the notion of risk loses its moral neutrality and, paradoxically, its statistical validity, when 'the acceptance of solidarity is accompanied by a demand for control over personal behaviour.'[83] The current support for 'active social policy' epitomizes this 'moralizing' tendency, as it explicitly 'stresses the importance of shifting the focus of social programmes from insuring individuals against a few, well-defined contingencies towards investing in their capabilities and making use of them to the best of their potential at every stage of the life course.'[84] Governance through the concept of risk dissuades individuals from making claims on collective public or private pools and rather focuses on what they might change in their lifestyle, diet, professional activity and leisure so as to minimise their risks. Governing through risks absolves economic, social and political institutions from their responsibility in engendering diseases and disabilities, but requires pervasive systems of surveillance to be implemented.

Why do we fear (public and private) surveillance? In *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, David Brin[85] argues that the generalization of observation and surveillance, instead of constituting a threat for our fundamental rights and freedoms, may bring even greater freedom, total transparency of every-one to every-one being the only way to guarantee liberty *provided that the power of observation and surveillance be shared by us* all rather than only by the police, the wealthiest or the most powerful. Thought-provoking as he may be, Brin nevertheless pointed to a fundamental reason why surveillance as it is now developing in public and private spaces is frightening: information about others provides, to the person who controls that information, much power over those others. Privacy, in this view, is thus not so much about protecting a subjective sense of intimacy or of decency as it is about preventing situations where those who know things about others that not everybody knows be allowed, due to their privileged position in the information economy, to take advantage of the power this situation provides them to constrain others. I will return to that later. Either increased privacy or total transparency can guarantee against that threat, as total transparency of everyone to everyone would suppress the differential op power assigned by access to restricted knowledge. Gillom provided a very useful analysis of the effects of surveillance. According to him, the effects of surveillance include:"degradation, the loss of control, the implied suspicion, the feelings of being just a number, the anxiety over errors or subterfuges being caught, the fear of malevolence or

[83] Pierre Rosanvallon, *La nouvelle question sociale. Repenser l'État providence*, Seuil, 1995.
[84] Organisation for Economic Cooperation and Development (2005) Extending Opportunities: How Active Social Policy Can Benefit Us All, OECD.
[85] In *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Perseus Books Group (1999).

incompetence on the part of surveillance practitioners, the fear of breaking rules or departing from norms that are unknown, and, especially, the need or desire to break the rules."[86]

The fact that the information society takes the orientation of a surveillance society is not a spontaneous phenomenon, nor the unpredictable result of scientific progress, but epitomizes the phenomenon of co-production between technology and society, notably popularized by Sheila Jasanoff.[87] Acknowledging that science, business, and politics are not separated spheres of human activity, but are rather interacting indistinctively in our collective 'social metabolism', increases the necessity that the material, cultural, social and political conditions of the democratic process be present from the beginning in the design of techno-scientific development.

II.1.2.2. Reassessing the normative grounds for privacy.

Strong privacy-adverse reasoning in contemporary society makes the need to ground privacy on strong normative grounds more crucial than ever. I would like to reassess those grounds on the basis of what I have already suggested about the intimate link between privacy and individual and political autonomy. In such a view, privacy appears as a precondition to the meaningful exercise of most other fundamental individual attributes and capabilities, such as human dignity and individual autonomy, and as a social structural instrument aimed at fostering social justice, democracy and the other values which our Western democracies are supposed to praise so much.

John Dewey argues that rights need not be justified as the immutable possession of the individual, but as instrumental in light of 'the contribution they make to the welfare of the community'.[88] Rather than merely a tool for the realisation of individual liberties (agent-relative values), privacy (thoroughly conceived to take into account the complex and heterogeneous meanings of private information) may be an essential structural tool, for the preservation of autonomous individuals empowered with the contestation (and reconstitution) abilities (typically agent-neutral values) needed in order to negotiate a new social contract on the threshold of an information era characterized by the possibility of

[86] John Gilliom, *Overseers the Poor*, Chicago University Press, 2001, p. 125.
[87] Sheila Jasanoff, *States of Knowledge: The Co-Production of Science and the Social Order*, Routledge, 2004.
[88] John Dewey, « Liberalism and Civil Liberties » in *John Dewey: The Later Works*, 1925-1953 : 1938/Logic: The Theory of Inquiry, Vol. 12, Boydston, J A (ed.), Southern Illinois University Press, 1991, p. 374.

refining, in an exponential manner, the classification of people in categories of risks, merits, abilities, etc.[89]

As already suggested, privacy (as 'insulation') guarantees the possibility for the subject to think differently from the majority and to revise his first order preferences. Thus, privacy is a condition for the existence of 'subjects' capable of participating in a deliberative democracy. As a consequence, privacy also protects lawful, but unpopular, lifestyles against social pressures to conform to dominant social norms. Privacy as freedom from unreasonable constraints in the construction of one's identity, serves to prevent or combat the "tyranny of the majority". The right to privacy and the right not to be discriminated against have in common that they protect the opportunities, for individuals, to experiment a diversity of non-conventional ways of life.[90] Privacy is itself a tool for preventing invidious discriminations and prejudices.

Strahilevitz recently argued against this position that there is often an essential conflict between information privacy and antidiscrimination principles, as non-disclosure of pertinent information about a job applicant such as their criminal history induce employers to rely more heavily on distasteful statistical discrimination strategies:

"In the information age, we should consider approaching the statistical discrimination problem (…) using the government to help provide decision makers with something that approximates complete information about each applicant, so that readily discernable facts like race or gender will not be overemphasized and more obscure but relevant facts, like past job performance and social capital, will loom larger."[91]

Yet, the argument is easily dismissed: nothing indeed guarantees that information about past diseases, records of past convictions, etc. are in any way relevant to assess the job applicant's suitability for the job. As a consequence, it is

[89] In the same sense, see Paul De Hert and Serge Gutwirth, « Privacy Law, Data Protection and Law Enforcement. Opacity of the individual and Transparency of Power", in. Eric Claes and Serge Gutwirth, eds., *Privacy and the Criminal Law*, Intersentia, 2006, pp.61-101.

[90] See particularly Charles Fried, "Privacy: a moral analysis.", *Yale Law Journal,* 1968, 77:475-93, arguing that informational privacy rights serve to free us "to do or say things not forbidden by the restraints of morality, but which are nonetheless unpopular or unconventional." In that sense, the right to privacy as guaranteed in Article 8 of the European Convention on Human Rights has been interpreted as implying the right, for people belonging to the Tzigan community, to live in caravans, such way of life being constitutive of the Tzigan way of life, that has to be respected as part of their right to private and family life. See Coster v. United Kingdom (n°24876/94) and Chapman v. United Kingdom (n°27238/95) of January 18, 2001. The European Court on Human Rights has also acknowledged that failure to legally acknowledge the new sexual identity of a trans-sexual person constituted a violation of her right to privacy. See I v. United Kingdom (requête n° 25680/94) of July 11, 2002.

[91] Lior Jacob Strahilevitz, "Privacy versus Antidiscrimination", *Chicago Law & Economics Working Paper*, No. 349 (2D Series), July 2007.

most probable that more information would increase the reach of the employer's prejudices much more than it would increase a job applicant's opportunities.

The rationale grounded on prevention of discrimination for constraints imposed on the free trade of personal information between concerned persons and their employers, insurers and other interested third parties is much challenged, however, especially in the United States. In neo-rule-utilitarian reasoning[92], economic efficiency may be considered as the final value, the prevention of discrimination then being instrumental and contingent to realizing efficiency.[93] Those debates attest to a fundamental ambiguity inherent to human rights discourses, an ambivalence between two conceptions of individual liberty, the roots of which have been located in the Anglo-American and the European traditions respectively.

Privacy may moreover be necessary to guarantee a certain level of distributive justice, by maintaining of a certain degree of information asymmetry. Information asymmetries may be necessary to prevent "rational" discrimination that would deprive some individuals from access to basic goods such as subsistence food, healthcare and insurance. The perspective of 'dynamic pricing' for essential goods is incompatible with common views about justice and fairness. This substantiates our claim that, contrary to the frequent assertion, the 'opacity' of individual subjects may be, as much or even, in some circumstances, more favourable to the common good.

That leads us to the consideration that will introduce the next section: private information is power, and the normative ground of data protection is the balancing of power between data controllers and data subjects.

II.2 -The right to data protection.

II.2.1. Are potential application scenarios of AmI in the scope of application of the data protection directives?

The questions one needs to reflect on regarding "personal data" include the following. Can we value "personal information" as we value 'other' commodities (as 'law and economics' scholars would have it)? Should "personal information" rather be analyzed in terms of the power it confers to those in control of it (as the European data protection directives suggest)? Is some "personal information" so closely related to the individual's personality that some measures of inalienability should be enforced? Or are there other reasons, related to the public's interest, that would require the implementation of strong legal restrictions on the

[92] Rule utilitarianism requires not that individuals maximize welfare as they act, but rather that they conform their acts to rules that maximize welfare.
[93] Richard W. Wright, "The Principles of Justice", *Notre Dame Law Review*, 2000, 75: 1859.

possibility for information to cross the former social and physical borders that guaranteed the 'impermeability' of social microcosms? More importantly, for our immediate purpose, we should assess whether the European Data Protection directives are indeed applicable in a context of AmI.

The Directive 95/46/EC only applies to processing of *personal data,* which it defines, as

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

The concept of personal data has recently been elucidated by the Article 29 Working Party on the protection of personal data[94], according to which the concept of personal data refers to:

- "*any information*", either objective (such as the substances in one's blood) or subjective (such as opinions or assessments), either correct or incorrect, about individuals, regardless of their position or capacity (as consumer, patient, employee, etc.), and regardless of the format or medium on which that information is contained (numerical, graphical, photographical, acoustic);

- that *relates*, even indirectly, *to individuals* (information on the functioning of a machine where human intervention is required and allowing to ascertain the productivity of the person working on that machine, or information about the length and pace of a queue, allowing to ascertain the productivity of an employee in an office or a shop),[95] either because it contains information about a particular person, and/or because that information is processed for the purpose of evaluating, treating in a certain way or influencing the status or behaviour of an individual, and/or because the processing of that information is likely to have an impact on a certain person's rights and interests (the mere fact that the individual could be treated differently from others as the result of the processing of the data counts as "impact" in this regard), taking into account all the circumstances surrounding the case.

This broad understanding of the concept of *personal data* is not unanimously endorsed in all the countries of the European Community. For example, although the French law of August 2004 defines personal data as: "toute

[94] Working Party on the Protection of Individuals with regard to the Processing of Personal Data (WP29), Opinion on the concept of personal data, WP 136 of 20th June 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

[95] The WP29 had previously noted, in the context of its discussion on the data protection issues raised by RFID tags, that "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated." (Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005, p. 8.)

information relative à une personne physique qui peut être identifiée, directement ou indirectement, par reference à un numéro d'identitification, ou à un ou plusieurs elements qui lui sont propres".[96] However, in the UK, the concept of personal data has been interpreted more restrictively by the Court of Appeal's 2003 decision in *Duran v. FSA* (a case about disclosure of information in the financial service sector), restricting the meaning of "personal data" to information that is "biographical in a significant sense, that is, going beyond the recording of the putative data subject's involvement in a matter or event that has no personal connotations".[97] How the interpretation by the Article 29 Working Party will impact of future interpretation of the applicability of the directive in a world of ambient intelligence remains to be seen.

Another issue relates to the category of *sensitive data*. Although, by default, the European Data Protection framework organizes the "transparency" of personal information, designing rules for the processing of personal data, some types of personal data, that the directive qualifies as *sensitive data*, are excluded from the framework and may never be processed. In principle, Article 8 of the Directive 95/46/EC makes it illegal to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.[98] This raises particular

[96] Article 2 al. 2 Law of 6 January 1978 modified in august 2004.

[97] Duran v. FSA, [2003] EWCA Civ 1746 (§28). See L. Edwards, "Taking the "Personal" Out of Personal Data: Duran v. FSA and its Impact on Legal Regulation of CCTV", *SCRIPT-ed*, 1(2), 2004 http://www.law.ed.ac.uk/ahrc/script-ed/issue2/durant.asp

[98] Article 8 The processing of special categories of data:

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that' the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3.Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of

questions with regards to some of the potential AmI applications, as the intervention of information technologies may alter the 'nature' of the data involved. Images of persons unavoidably provide information about their racial or ethnic origin; profiling of persons on the basis of their preferred entertainment programs in a context of interactive web TV may carry indications about those persons' political opinions, religious or philosophical beliefs; tracking of consumers' choices in a supermarket may reveal sensitive aspects of their private life: a specific diet may indicate religious beliefs, buying drugs (supermarkets increasingly sell health products and medicines) may indicate one's health status, etc.

II.2.2. Are the technical visions of AmI compatible with the fundamental principles of data protection?

The prospect that ubiquitous, proactive computing systems will 'spontaneously' respond to individual 'needs' in adapting the environment and the systemsthemselves without the individual having to decide anything anymore about that, and that those systems will become so embedded in daily lives that they will literally 'disappear' from users' consciousness[99], so that individuals will not even necessarily be conscious of their presence, promises important disturbances for our perception and implementation of individual informational rights and data controllers' responsibilities.

Article 6 of the Directive 95/46/EC specifies the requirements relating to the *data quality*:

---

health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph I provided for in paragraphs 4 and 5 shall be notified to the Commission

Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

[99] Mark Weiser, "Computer Science Problems in Ubiquitous Computing", *Commun.*, *ACM 36*, ACM Press, 1993, 7: 75-84.

1.Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2.It shall be for the controller to ensure that paragraph 1 is complied with.

According to the requirements relating to data quality thus, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. How can the legitimacy of the undescribed finality of the data processing, and the compatibility of further uses of the data with those initial finalities be assessed even though the technology may give birth to indeterminate and currently unforeseeable applications and although service providers may assume different functions?

Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The directive also requires that processed personal data be accurate and, where necessary, kept up to date; and that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Those principles are arguably difficult to comply with when the purpose for which the data are collected, and for which they may be further processed, are so difficult to define *a priori* as they are in AmI systems. What about that principle of data minimization in emerging AmI information systems where, by default, everything is recorded?

Article 7, relating to the criteria for assessing the *legitimacy* of personal data processing reads as follows:

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Whenever the technologies involved fade out of the user's consciousness, what happens to the traditional, and legal, requirement that individuals give their "informed consent" to any processing of their personal data? Would *implicit* consent, implied from the individual's use of an infrmation system or acceptance of benefits from that system, be enough to protect the fundamental rights, freedoms and interests of individuals? What is the impact of the "performativity" (such as the impact of autonomic profiling on users' personality) of technologies on the validity of individual consent?

Further, requirements of the directive regarding *transparency* of the processing of personal data (Article 10 and 11) will not be easy to fulfill either in the context of AmI. Article 10 requires the controller or his representative to provide a data subject, from whom data relating to himself are collected, with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such asthe recipients or categories of recipients of the data;whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11 provides that

where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such asthe categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

In sum, invisibility of the terminal in AmI systems, and the inclusion of decentralized and multilateral service models, are *de facto* incompatible with the principle of transparency.

Moreover, the question remains how responsibility could be assigned in a system of (human-computer) distributed agency. The recent massive personal data losses in the UK and elsewhere, as well as the fact that "biased computer systems are instruments of injustice",[100] epitomize the crucial necessity of rethinking issues of responsibility in networked digital environments.

Finally, to the extent that data protection is meant, as it is at least in part, to protect people's privacy, it is necessary for it to be an effective means to indeed protect individual privacy, for users to implement the rights provided by the EU Data protection scheme, including the rights provided by **Article 12** of the Directive 95/46/EC. Unfortunately, very few users take the opportunity to genuinely control and intervene in the processing of their personal data as the European data protection framework allows them to do. One may think of several reasons for this.

First, most peoples' perceptions of what their right to privacy is about correspond to the traditional theories of privacy as protecting intimate and/or sensitive information. Information that they do not subjectively perceive as intimate and/or sensitive is not, in most persons' minds, anything that they should worry about disclosing or being processed by others. That traditional conception does not necessarily fit the new configuration of socio-technical constellations involved in an AmI world, where what privacy advocates are worried about is collection, use and disclosure of information that is not sensitive nor intimate *per se*, and that is increasingly collected in public. As Nissenbaum relevantly

[100] Batya Friedman, Helen Nissenbaum, « Bias in Computer Systems », *ACM Transactions on Information Systems,* Vol. 14, No. 3, July 1996, Pages 330 –347.

argued[101]: the challenge that information technology raises for our traditional conceptions of privacy results from both the fact that information technologies allow the use of information gathered in one specific context to move outside that context more easily than ever, and from the ever increasing capacity to aggregate (even trivial and non intimate nor sensitive) information about a person to an extent that very precise knowledge is gained about that person.

Another reason why people do not exercise their data protection rights is that, in the short term, when disclosing personal data is rewarded with immediate utilities, advantage or privileges in their interaction with other agents such as a supermarket, a trader or a service supplier on the internet, keeping control of their own personal data may appear immaterial to them compared to the immediate and tangible advantages of waiving such control.

That brings us back to an important, yet under discussed issue: the normative value of personal information. Can personal information be conceived as pure commodity? Or should one acknowledge that personal information is among those new "hybrid" objects[102] that modernity has produced, half way between the category of "subjects" and the category of "objects", and therefore deserving an *ad hoc* legal status. Such a legal status would not go as far as borrowing the inviolability and inalienability that attach to the rights which protect the dignity of human beings, yet cannot be considered either as fully alienable commoditized consumption goods. Personal information emanates from, and contributes to the formation of individual personality, and has therefore to do with human dignity, yet, a person is obviously irreducible to 'his' personal information, which is 'an aspect of the identity' she 'projects to the world', in the inspiring words of Philip Agre that opened our reflexions.

CONCLUSIONS

This article's prospective focus is on two unprecedented challenges brought by the announced recent evolution of the information society. First, it argues, data mining and profiling processes inherent to the new 'services' offered or to be offered to citizens and consumers in the advanced information society, as well as the intensification of automated surveillance and scrutiny, may well interfere with the individual's self-formation (or subjectivation), chanelling his or her behaviours, preferences, thoughts, emotions and choices, and jeopardising their

[101] Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy*, 17, 1998, p. 559.

[102] About the modern « hybrids », see Bruno Latour, *Nous n'avons jamais été modernes. Essai d'anthropologie symétrique*, La Découverte/Poche, 1991. On the idea of 'incomplete commodification', see Margaret Jane Radin, *Contested Commodities,* Harvard University Press, 1996.

genuine capacity for individual reflexive self-determination and collective deliberation. Second, the article tentatively explores some of the issues that would arise from the gradual 'spread' of agency in 'ambient intelligence networks', whereas our traditional, and legal, conception of agency presupposes the individual human subject to be the exclusive locus of agency. Both of these specific challenges concern the more general paradox that whereas the figure of the individual, the sovereign subject, autonomous, rational and responsible, is considered a 'given', pre-existing reality, a basic unit of neoliberal modes of governance, the technological and socio-political developments of the information society challenge, quite radically, the classical Enlightenment notion of the sovereign subject.

Having assessed the normative grounds of privacy and data protection, the paper has established that those rights are not only valuable for the reason that they preserve and/or advance the interests of the individual rightholders, but also have a fundamentally collective, democratic dimension, or a "social-structural" value. The right to privacy protects the legal subject's legitimate interests in controlling aspects of his or her identity and personality that he or she projects on the world, and in being free from unreasonable constraints on the construction of his identity. But the right to privacy also preserves the possibility for the legal subject to develop as an autonomous citizen, endowed with the reflexive capability needed in order to usefully participate in the processes of deliberative democracy; whereas data protection and rules of non disclosure of personal data avoid the creation or perpetuation of situations of domination and oppression. The collective, social-structural dimension of privacy and data-protection is intimately linked with the 'justiciability' of knowledge that AmI systems construct over and about individuals.

The role of the law, despite its weakness to address the unprecedented challenges that the technical visions of AmI present, is to allow and protect the possibility of democratic debates, involving all stakeholders, about the issues involved. It is exactly here that the morality of the law resides.[103] This may require legal intervention to prevent power imbalances among the stakeholders. This may also require legal intervention to protect, up to a certain extent,

[103] In that sense, see Jacques Derrida, *The Force of Law* in *Deconstruction and the Possibility of Justice*, Cornell, D, Rosenfield, M and Gray, D (eds), Routledge, 1992. Derrida, like Foucault, considers that the law is never impartial but always results from, and carries, strategies of power. Yet, where Foucault situates the possibility of resistance *within* the productive power of normativity and governmentality, Derrida argues that the law must be transposed from that sphere of normativity and governmentality, where it functions as "droit", and rethought in relation to an impossible justice. See also Margrit Shildrick, "Transgressing the law with Foucault and Derrida: some reflections on anomalous embodiment", *Critical* Quarterly, Vol. 47, n. 3, Autumn 2005, pp. 30-46. See also Colin Perrin, "The Silent Responsibility of Law", *International Journal for the Semiotics of Law / Revue Internationale de Sémiotique Juridique* Vol. XI no.31, 1998, 39-47.

individual choices and preferences from the tyranny of the majority. The European privacy data protection framework also assigns a crucial mandate to the law: the mandate of balancing the competing interests at play. In order to fulfill its task, the law therefore needs first to have these interests identified and their legitimacy assessed.[104] An urgent task of the State is to give a voice to the variety of stakeholders, identify their respective visions and interests, and organize a discussion process to ensure that the information systems remain compatible with the democratic character of our society and with the fundamental values attested in our attachment to citizens' fundamental rights and liberties.

It is the law's communicative function (which is highly complex, and that we have, in this paper, modestly tried to fulfill in part) to create a normative framework, a vocabulary to structure normative discussions, as well as institutions and procedures that promote further discussion. The law also has a related expressive function to clarify which fundamental standards and which values are important. Finally, confronted to unprecedented social and political challenges, a fundamental role of the law is to evolve so as to ensure that we remain in a free and democratic society. The changes needed now are, first, acknowledging the inability of law alone to guarantee what really matters about privacy and data protection in the context of AmI. Second, 'delegating' some of its power to the designers of the technologies, who, for a large part, have *de facto* gained the power to shape the infrastructure of the public space.[105] Technology designers, as well as the industrial sector, should therefore, more than they do today, realize how accountable they are towards the general public and towards the democratic institutions. The time has come to begin, at last, a long awaited interdisciplinary discussion.

[104] Proecedural safeguards, such as the requirements of transparency and accountability are obviously insufficient to establish the legitimacy of certain surveillance practices in society, especially in the field of law enforcement. (De Hert, P., Gutwirth, S., « Privacy Law, Data Protection and Law Enforcement. Opacity of the individual and Transparency of Power", in. Eric Claes and Serge Gutwirth, eds., *Privacy and the Criminal Law*, Intersentia, 2006, pp.61-101.)

[105] Value sensitive design such as that exhibited in privacy enhancing technologies is indeed much encouraged by European policy makers. See for example the Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions on « Radio Frequency Identification (RFID) in Europe: Steps towards a Policy Framework » COM(2007)96.

References

Agre, P.E, Rotenberg, M., (eds*.), Technology and Privacy. The New Landscape*, MIT Press, 1998.

Akrich, M., "The De-Scription of Technological Objects", in. W.E. Bijker and J. Law, *Shaping Technology / Building Society*, MIT Press, 1992.

Austin, L., "Privacy and the Question of Technology", *Law and Philosophy*, 22, 2003, pp. 119-166.

Baker, C. E., "Posner's Privacy Mystery and the Failure of Economic Analysis of Law", *Georgia Law Review*, 1978, 12(3): 475-496.

Brin, D., *Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Perseus Books Group, 1999.

Callon, M., "Les réesaux sociaux à l'aune de la théorie de l'acteur-réseau", *Sociologies Pratiques*, n.13, pp. 37-43, 2006.

Campbell, A.V., "The Ethical Challenges of Genetic Databases: Safeguarding Altruism and Trust", *King's Law Journal*, 2007, 18, pp. 227-245: 241.

Cohen, J.E., « Privacy, Ideology, and Technology: A Response to Je rey Rosen », *Georgetown Law Journal*, 2001, 89 : 2029-2045.

Constitution Project's Liberty and Security Committee (USA) Guidelines for Public Videosurveillance: A guide to Protecting Communities and Preserving Civil Liberties, 2007, www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf.

Custers, B., *The Power of Knowledge, Ethical, Legal, and technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, 2004.

De Hert, P., Gutwirth, S., « Privacy Law, Data Protection and Law Enforcement. Opacity of the individual and Transparency of Power", in. Eric Claes and Serge Gutwirth, eds.,*Privacy and the Criminal Law*, Intersentia, 2006, pp.61-101.

Dempsey, J.X., Rubinstein, I., "Lawyers and Technologists. Joined at Hips*?", IEEE Security and Privacy*, May/June 2006, pp. 15-19.

Derrida, J., "The Force of Law" in Cornell, D, Rosenfield, M and Gray, D (eds), *Deconstruction and the Possibility of Justice*, Routledge, 1992.

Dewey, J., "Liberalism and Civil Liberties", in Boydston, J A (ed.), *John Dewey: The Later Works, 1925-1953 : 1938/Logic: The Theory of Inquiry*, Vol. 12, , Southern Illinois University Press, 1991.

Dinant, J.-M., Lazaro, C., Lefever, N., Poullet,Y., Rouvroy, A., "L'application de la Convetion 108 au mécanisme de profilage", Report for the Council of Europe, 2007.

Dworkin, G., *The Theory and Practice of Autonomy*, Cambridge University Press, 1988.

Edwards, L., "Taking the "Personal" Out of Personal Data: Duran v. FSA and its Impact on Legal Regulation of CCTV", *SCRIPT-ed,* 1(2), 2004 http://www.law.ed.ac.uk/ahrc/script-ed/issue2/durant.asp (accessed on January 25, 2008).

Epstein, R., "Deconstructing Privacy and Putting it Back together Again", *Social Philosophy and Policy,* 2000, 17(2), p. 22.

Epstein, R., "How Much Privacy Do We Really Want?", *Hoover Digest*, 2002.

European Commission for Democracy Through Law (Venice Commission), Opinion on videosurveillance in public places by public authorities and the protection of Human Rights, of 23 March 2007 (Study No. 404/2006), CDL-AD(2007)014, http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.pdf

European Data Protection Supervisor, Opinion on the communication from the Commission to the European Parliament, the Council, the European economic and Social Committee and the Committee of the Regions on « Radio Frequency Identification (RFID) in Europe: Steps towards a Policy Framework » COM(2007)96.

European Network of Excellence FIDIS (Future of Identity in the Information Society)'s study on "Radio Frequency Identification (RFID), Profiling, and Ambient Intelligence (AmI)", http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf

Faiden, R., Beauchamps, T., A, *History and Theory of Informed Consent*, Oxford University Press, 1986.

Farnsworth, W., "The Taste for Fairness", *Columbia Law Review*, 2002, 102, pp. 1998-2010.

Fisk, C. L., "Reflections on the New Psychological Contract and the Ownership of Human Capital", *Connecticut Law Review*, 2002, p. 34 : 765-782

Flemming, J.E., "Securing Deliberative Autonomy*", Stanford Law Review*, Vol. 48, N.1, 1995, pp. 1-71.

Flemming, J.E., "Securing Deliberative Democracy", *Fordham Law Review*, Vol. 72, p. 1435, 2004.

Foucault,M., *L'herméneutique du sujet*, Cours du collège de France,1981-1982, Seuil / Gallimard, 2001.

Franko Aas, K., " 'The body does not lie' : Identity, risk and trust in technoculture", *Crime, Media, Culture*, 2006, 2(2) :143-158.

Fried, Ch., "Privacy: a moral analysis.", *Yale Law Journal*, 1968, 77, pp. 475-93.

Friedewald, M., Vildjiounaite, E., Punie, Y., and Wright, D., "Privacy, identity and security in ambient intelligence: A scenario analysis.", *Telematics and Informatics*, 2007, 24(1), p.15.

Friedman, L., *Law and Society. An Introduction*, Prentice Hall, 1977.

Friedman, B., Nissenbaum, H, « Bias in Computer Systems », *ACM Transactions on Information Systems*, Vol. 14, No. 3, July 1996, Pages 330 –347.

Gavison, R., "Privacy and the Limits of Law" in Schoeman, F D (ed.), *Philosophical Dimensions of Privacy: an Antology*, Cambridge University Press, 1984.

Gilliom, J., *Overseers the Poor*, Chicago University Press, 2001.

Goldman, E., « Search Engine Biases and the Demise of Search Engine Utopianism », *Yale Law Journal of Technology*, 2006, 188-200.

Gutwirth, S., De Hert, P., "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Claes, E., Duff, D. and Gutwirth, S., *Privacy and the Criminal Law*, Intersentia, 2006.

Habermas, J., *Between Facts and Norms*, MIT Press, 1996.

Hacking, I., "Making Up People*", London Review of Books*, 26(16), 17 August 2006.

Haraway, D. J., *Modest_Witness@Second_Millenium. FemaleMan_Meets_OncoMouse: Feminism and Technoscience*, Routledge, 1997.

Hardt, M. et Negri, A., *Multitude. Guerre et démocratie à l'âge de l'empire*, La Découverte, 2004.

Hildebrandt, M., "Profiles and Correlatable Humans", in: Henning, Ch., Stehr, N. and Weiler, B., (eds.), *Knowledge and the Law. Can Knowledge be Made Just?*, New Jersey: Transaction Books 2007.

Hilty et al.,*The Precautionary Principle in the Information Society – Effects of Pervasive Computing on Health and Environment*, Swiss Center for Technology Assessment (TA-SWISS), Bern (TA46e/2005).

IBM, Autonomic computing manifesto. http://www.research.ibm.com/autonomic/manifesto/

Institute for Prospective Technological Studies – Joint Research centre, Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS Technical Reports Series, EUR 20823 EN, 97.

Jacobs, A., "The benefits of The Legal Analytic Perspective For esigners of Context-Aware Technologies", http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/ (accessed on January 25, 2008)

Jasanoff, S., *States of Knowledge: The Co-Production of Science and the Social Order*, Routledge, 2004.

Kronman, A.T., "Paternalism and the Law of Contracts", *Yale Law Journal*, 1983, 92, p. 770.

Latour, B., *Nous n'avons jamais été modernes. Essai d'anthropologie symétrique*, La Découverte/Poche, 1991.

Latour, B., *Reassembling the Social: An Introduction to Actor-Network-Theory*, Oxford University Press, 2005.

Lefebvre, H., *The Production of Space*, Blackwell, 1991.

Lessig, L., "The Architecture of Privacy", *Vanderbilt Entertainment Law and Practice*, 1, 1999

Lessig, L*., Code and Other Laws of Cyberspace*, Basic Books, 1999.

Lyon, D*., The Electronic Eye: the Rise of Surveillance Society*, University of Minnesota Press, 1994.

McGrath, J.E., *Loving Big Brother: Performance, Privacy, and Surveillance Space*, Routledge, 2004.

Mill, J.S*., On Libety*, Cambridge University Press, 1989 [1859].

Miller, T., "Testimony on Genetic privacy, before the House Judiciary Subcommittee on the Constitution on genetic privacy", September 12, 2002. http://www.house.gov/judiciary/miller091202.htm#_edn11>

Mumford, L., « Authoritarian and Democratic Technics », *Technology and Culture*, 5(1), 1964, 1-8.

Nickel, R., "Jürgen Habermas' concept of co-originality in times of globalization and the militant security state*", IUE Working Paper Law*, 2006/27.

Nissenbaum, H., "Protecting Privacy in an Information Age: The Problem of Privacy in Public", *Law and Philosophy*, 17, 1998, p. 559.

O'Neill, O., *Autonomy and Trust in Bioethics* (Gifford Lectures, 2001), Cambridge University Press, 2002.

Organisation for Economic Cooperation and Development, Extending Opportunities: How Active Social Policy Can Benefit Us All, OECD, 2005.

Perri6*, Private Life and Public Policy in The future of Privacy: Public Trust in the Use of Private Information* v. 2, Lasky, K and Fletcher, A (eds), Demos Medical Publishing, 1998.

Perrin, C., "The Silent Responsibility of Law", *International Journal for the Semiotics of Law / Revue Internationale de Sémiotique Juridique* Vol. XI no.31, 1998, 39-47.

Planetary Collegium / Montreal 2007 Summit, "Reviewing the Future: Vision, Innovation, emergence", 19-22 April 2007 http://summit.planetary-collegium.net/abstracts.html

Posner, R. A., "An Economic theory of Privacy" in Schoeman, F. D., (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

Posner, R. A., "The Right of Privacy", *Georgia Law Review*, 12: 393-422, 1978.

Poullet,Y., Rouvroy, A., Darquennes, D., « Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID », *Cahiers droits, science et technologie*, CNRS, forthcoming 2008.

Poullet, Y., Dinant, J-M., "The internet and private life in Europe: Risks and aspirations", in. *New Dimentions of Privacy Law*, Cambridge University Press, 2006, pp. 60-90.

PRIAM (privacy issues in ambient intelligence) project funded by the French INRIA.http://priam.citi.insa-lyon.fr/index.php?option=com_content&task=view&id=12&Itemid=26

Radin, M.J., *Contested Commodities*, Harvard University Press, 1996.

Rosanvallon, P., *La nouvelle question sociale. Repenser l'État providence*, Seuil, 1995.

Rosen, J. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Random House Trade Paperback, 2005.

Rouvroy, A., Poullet, Y., « The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy. », in *Reinventing Data-Protection ?*, proceedings of the International Conference held in Brussels, 12-13 October 2007, Springer (forthcoming).

Rouvroy, A.,*Human Genes and Neoliberal Governance: A Foucauldian Critique*. Abingdon [England] & New York: Routledge-Cavendish, 2008.

Schoeman, F., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

Schwartz, P.M., "Beyond Lessig's Code for internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices", *Wisconsin Law Review*, 2000, 743-788.

Schwartz, P.M., Treanor, W.M., "The New Privacy", *Michigan Law Review*, 2003, 101.

Shildrick, M., "Transgressing the law with Foucault and Derrida: some reflections on anomalous embodiment", *Critical Quarterly*, Vol. 47, n. 3, Autumn 2005, pp. 30-46.

Skordas, T. and Metakides, G., "Major Challenges in Ambient Intelligence", *Studies in Informatics and Control*, 12(2), June 2003.

Solove, D., Rotenberg, M., and Schwartz, P.M*., Privacy, Information and Technology*, Aspen Publishers, 2006.

Solove, D., *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2006.

Spiekermann, S., Pallas, F., "Technology paternalism – wider implications of ubiquitous computing", *Poiesis Prax*, 4, 2006, 6-18.

Spielmann, D., "Jurisprudence des jurisdictions de Strasbourg et de Luxembourg dans le domaine des droits de l'homme: conflits, incohérences et complémentarités", in. Alston P. (ed.), *L'Union Européenne et des Droits de l'Homme*, Bruxelles, Bruylant, 2001.

Strahilevitz, L.J., "Privacy versus Antidiscrimination*", Chicago Law & Economics Working Paper*, No. 349 (2D Series), July 2007.

Suchman, L., *Human-Machine Reconfigurations : Plans and Situated Actions*, Cambridge University Press, 2d.ed., 2006.

SWAMI (Safeguards in a World of Ambient Intelligence) project, pubished as Wright, David, Serge Gutwirth, Michael Friedewald et al., *Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.

TAUCIS (Technology Assessment of Ubiquitous Computing and Informational Self-Determination) project, funded by the German Federal Ministery for Education and Research, http://www.taucis.hu-berlin.de/content/de/ueberblick/english.php,

Warren, S., Brandeis, L., "The Right to Privacy", *Harv. L. Rev*. 1890.

Wei, S.X., "Poetics of performative space", *AI & Society*, 21(4), June 2007.

Weiser, M., "Computer Science Problems in Ubiquitous Computing", *Commun., ACM 36*, ACM Press, 1993, 7, pp. 75-84.

Werbach, K.D., "Sensors and Sensibilities", *Cardozo Law Review*, 2007, 28(5) : 2321-2372.

Westin, A.F.*, Privacy and Freedom*, Athenaeum, 1967.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Group 29), Working document on data protection issues related to RFID technology, WP 105, of 19th January 2005, ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Group 29), Opinion on the concept of personal data, WP 136 of 20th June 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Group 29), Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, of 28th June 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Group 29), Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp90_en.pdf

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Group 29), Opinion on the Processing of Personal Data by means of Video Surveillance of 11th February 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf

Wright, R.W., "The Principles of Justice", *Notre Dame Law Review*, 2000, 75, p. 1859.

Wright, D., Gutwirth, S., Friedewald, M. et al.,*Safeguards in a World of Ambient Intelligence*, Springer, Dordrecht, 2008.